目　录

第一章　算术基本定理

除法算式

1．观察表 1.1．如果用同样的方法向下延续，它能否包含我们指定的任何一个正整数？

2．表 1.1 中的每个数与它下面的数有什么关系？

3．简洁地描述由 0 以下的一列数所组成的整个集合．

4．如果在 0 以下的一列中取两个数并把它们相加，那么它们的和必在表的哪一位置？

5．表 1.1 的整个排列可以看做是以 0 下面的一列数与表头上的三个数 1,2,3 下面的各列数的加法表．利用你对 0 以下的一列数的简单描述，对于由 1 以下的一列数所组成的整个集合，给出一个比较简洁的描述，并对由另外的两列数组成的集合也都给出类似的简洁描述．

6．如果两个数都在第二列，那么大数与小数的差在什么位置？

7．如果两个数都在第三列，那么大数与小数的差在什么位置？试用具有一般性的表示方法对于所有这种数对来证明你的结论．

8．如果两个数都在第四列，那么大数与小数的差在什么位置？证明你的结论．

9．如果从第二列中取两个数，那么它们的和在什么位置？一般地证明你的结论．

10．如果从第四列中取两个数，那么它们的和在什么位置？一般地证明你的结论．

11．有没有一般规则，可填出一列中的数与另一列（包括本列）中的数的加法表？如果在这个表中只用到各个列的表头上的数

表 1.1

0	1	2	3	0	1	2	3
4	5	6	7	100	101	102	103
8	9	10	11	104	105	106	107
12	13	14	15	108	109	110	111
16	17	18	19	112	113	114	115
20	21	22	23	116	117	118	119
24	25	26	27	120	121	122	123
28	29	30	31	124	125	126	127
32	33	34	35	128	129	130	131
36	37	38	39	132	133	134	135
40	41	42	43	136	137	138	139
44	45	46	47	140	141	142	143
48	49	50	51	144	145	146	147
52	53	54	55	148	149	150	151
56	57	58	59	152	153	154	155
60	61	62	63	156	157	158	159
64	65	66	67	160	161	162	163
68	69	70	71	164	165	166	167
72	73	74	75	168	169	170	171
76	77	78	79	172	173	174	175
80	81	82	83	176	177	178	179
84	85	86	87	180	181	182	183
88	89	90	91	184	185	186	187
92	93	94	95	188	189	190	191
96	97	98	99	192	193	194	195
				196	197	198	199

(0, 1, 2, 3)，那么所得到的表就是模 4 的加法表的一个例子，这样的表用 $(Z_4, +)$ 表示．

+	在0列中的数	在1列中的数	在2列中的数	在3列中的数
在0列中的数				
在1列中的数				
在2列中的数				
在3列中的数				

12. 表1.1中同一列中的两个数被称为对模4同余[①]. 我们记 $5 \equiv 13 \pmod 4$. 请你给出 $a \equiv b \pmod 4$ 的代数定义.

13. 每个正整数是否恰好能表示成四个形式 $4q, 4q+1, 4q+2, 4q+3$ 中的一个 ($q \geqslant 0$ 是某个整数)? 如何判断一个特定的数(例如1553)是这些形式中的哪一种?

14. 研究关于表1.1的列的乘法结果, 能否构造一个类似于上述加法表的乘法表?

15. 在表1.2中, 用五个列来列出正整数. 对于由每一列中的数所组成的集合, 给出一个一般性的描述.

① 见第二章问题4及其注. —— 译者注.

16.每个正整数是否恰好能表示成五个形式 $5q, 5q+1, 5q+2, 5q+3, 5q+4$ 中的一个($q \geqslant 0$ 是某个整数)? 如何判断一个特定的数 (例如 6666)是这些形式中的哪一种?

表 1.2

0	1	2	3	4	100	101	102	103	104
5	6	7	8	9	105	106	107	108	109
10	11	12	13	14	110	111	112	113	114
15	16	17	18	19	115	116	117	118	119
20	21	22	23	24	120	121	122	123	124
25	26	27	28	29	125	126	127	128	129
30	31	32	33	34	130	131	132	133	134
35	36	37	38	39	135	136	137	139	139
40	41	42	43	44	140	141	142	143	144
45	46	47	48	49	145	146	147	148	149
50	51	52	53	54	150	151	152	153	154
55	56	57	58	59	155	156	157	158	159
60	61	62	63	64	160	161	162	163	164
65	66	67	68	69	165	166	167	168	169
70	71	72	73	74	170	171	172	173	174
75	76	77	78	79	175	176	177	178	179
80	81	82	83	84	180	181	182	183	184
85	86	87	88	89	185	186	187	188	189
90	91	92	93	94	190	191	192	193	194
95	96	97	98	99	195	196	197	198	199

17. 做出模 5 的加法表与乘法表. 至少对每个表中的两个表值给出正规的证明.

18. 表 1.1 是用四个列来列出正整数,而表 1.2 是用五个列来列出正整数. 一般地,如果用 b 个列来列出正整数(包括数 0),那么,第一行是哪些数? 第一列是哪些数? 每个正整数是否可以表示成第一行中的一个数与第一列中的一个数的和? 如果整数 a 和 bq 在同一行,那么 bq ,$b(q+1)$及 a 这三个数之间有什么关系? 推出 $a=bq+r$,其中 $r=0$ 或 r是小于 b 的正整数.

19. 设 a 和 b 是正整数 ,q_1 ,q_2 ,r_1,r_2 都是正整数或零,而且 r_1 和 r_2 都小于 b . 再设 $a=bq_1+r_1=bq_2+r_2$. 证明 r_1 与 r_2 的差是 b 的倍数, 从而推出 $r_1=r_2$ 以及 $q_1=q_2$.

(问题 18 与 19 合在一起就给出了除法算式).

20. 在表 1.3 中,所有的列都从 0,1,2,3 这一行出发向上和向下双方延伸. 对由每一列中的数组成的集合给出一般性描述. 问题 11 中得到的列的加法表对向上延伸的列是否仍成立? 问题 14 中得到的列的乘法表对向上延伸的列是否仍成立?

21. 数 -161 属于表 1.3 的哪一列(假定已将它延伸)?

22. 在由整数组成的加法群 (Z, +)中,用 4Z 表示表 1.3 中第一列的数所成的子集,其它列中的数所成的子集则分别用 4Z+1,4Z+2 及 4Z+3 表示. 用群论的语言描述(Z , +)的这四个子集.

23. 试提出一个对于任何整数 a 和任何正整数 b 都适用的除法算式.

24. 验证你所提出的除法算式.

除法算式可说是同余算术的基础. 在本章的其余部分,我们将用它来证明关地自然数因数分解的一些基本性质. 在和 N 不同的某些数系中,有时也可以证明类似的除法算式,从而也可以推出因数分解唯一性定理 ,例如 ,见问题 5.53.

表 1.3

−100	−99	−98	−97
−96	−95	−94	−93
−92	−91	−90	−89
−88	−87	−86	−85
−84	−83	−82	−81
−80	−79	−78	−77
−76	−75	−74	−73
−72	−71	−70	−69
−68	−67	−66	−65
−64	−63	−62	−61
−60	−59	−58	−57
−56	−55	−54	−53
−52	−51	−50	−49
−48	−47	−46	−45
−44	−43	−41	−41
−40	−39	−38	−37
−36	−35	−34	−33
−32	−31	−30	−29
−28	−27	−26	−25
−24	−23	−22	−21
−20	−19	−18	−17
−16	−15	−13	−13
−12	−11	−10	−9
−8	−7	−6	−5
4	−3	−2	−1
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63
64	65	66	67
68	69	70	71
72	73	74	75
76	77	78	79
80	81	82	83
84	85	86	87
88	89	90	91
92	93	94	95
96	97	98	99

最大公约数与 Euclid 算法

25．对下面给出的两个数集链，指出沿箭头移动的规律，以及何时停止的规律：

$\{57,36\}\to\{21,63\}\to\{21,15\}\to\{6,15\}\to\{6,9\}\to\{6,3\}\to\{3,3\}=\{3\}$停止．

$\{98,175\}\to\{98,77\}\to\{21,77\}\to\{21,56\}\to\{21,35\}\to\{21,14\}\to\{7,14\}\to\{7,7\}=\{7\}$停止．

从$\{170,130\}$开始，照上面的模式，做出一个数集链．

26．如果 $a>b$，那么，按照问题 25 中的模式，$\{a,b\}$的后继者是什么？如果链是从两个正整数开始的，为什么在链中不会出现负整数和零？

27．用问题 25 中给出的第一个数集链，对下面的每个方程，找出一对整数 x,y：

$$57=57x+36y,$$
$$36=57x+36y,$$
$$21=57x+36y,$$
$$15=57x+36y,$$
$$6=57x+36y,$$
$$9=57x+36y,$$
$$3=57x+36y.$$

28．用问题25 中给出的第二个数集链，将数 175，98，77，21，56，35，14，7 都写成 $98x+175y$ 的形式，其中 x,y 是整数．

29．数集$\{57x+36y\mid x,y\in Z\}$是否构成 $(Z,+)$的子群？这个集合中的最小正数是什么？这个数的每一个倍数是否必在这个集合中？这个集合中的每个数是否必是这个数的倍数？

30．对于由数 57 和 36 所生成的 $(Z,+)$的子群给出一个简

单描述.

31. 数集 $\{98x+175y \mid x, y \in Z\}$ 是否构成 $\{Z, +\}$ 的子群? 这个集合中的最小正数是什么? 这个数的每一个倍数是否必在这个集合中? 这个集合中的每一个数是否必是这个数的倍数?

32. 对于由数 98 与 175 所生成的 $(Z, +)$ 的子群给出一个简单描述.

33. 对于由非零整数 a 和 b 所生成的 $(Z, +)$ 的子群, 给出一个公式化的描述.

设 d 是这个子群中的最小正整数, 说明 d 的每一个倍数必属于这个子群的原因.

假设这个子群中有一个数 c 不是 d 的倍数, 用除法算式证明这个子群必定包含一个比 d 小的正整数. 这个矛盾就证明了, 由 a 和 b 生成的 $(Z, +)$ 的子群实际上是由一个数 d 生成的.

34. 设 a 与 b 是非零整数, 而且它们所生成的 $(Z, +)$ 的子群是由一个正整数 d 所生成的, 说明为什么有

$$d \mid a \text{ 和 } d \mid b$$

(d 整除 a 和 d 整除 b, 或者说, d 是 a 的因数和 d 是 b 的因数). 再回到对于由 a, b 所生成的子群的原始的描述, 证明: 对于某两个整数 x, y, 有 $d = ax + by$. 由此推出: a 和 b 的每一个公因数整除 d. 这说明 d 是 a 和 b 的最大的公因数, 即最大公约数, 记为 $d = \gcd(a, b)$.

35. 利用上题, 说明为什么必有整数 x, y, 使得 $2x+3y=1$. 根据经验, 找一对适合这个方程的整数.

设 $2a+3b=1$ 而且 $2c+3d=1$, 证明对于某个整数 t, 有 $2(a-c)=3(d-b)=6t$, 从而推出: $2x+3y=1$ 的每个解都是 $x=-4+3t, y=3-2t$ 的形式.

36. 证明整数集合 $\{12x+18y+27z \mid x, y, z \in Z\}$ 构成 $(Z, +)$ 的子群. 证明这个子群的每个元素都有因数 3. 通过适当选取 x, y, z,

证明 3 是这个子群的元素,从而推出这个子群是由 3 生成的循环群,而且 gcd (12,18,27) = 3.

37.对于由三个非零整数生成的 (Z,+)的子群,叙述并证明与问题 33 类似的结论.

38.对于三个非零整数的最大公约数,叙述并证明与问题 34 类似的结论.

39.在问题 25 中,用以寻求两个数的最大公约数的链通常简写为

{57, 36}→{36, 21}→{21, 15}→{15, 6}→{6, 3} 停止

与

{175, 98}→{98, 77}→{77, 21}→{21, 14}→{14, 7}停止.

这种形式称为 Euclid 算法.先写较大的数;当较小的数是较大的数的因数时,这过程停止.看看问题 25 中的哪些步骤在 Euclid 算法中被省略了.

40.用具有两个储存器的袖珍计算器,或两个计算器,或用笔和纸,计算 god (107360, 30866).

41.用除法算式描述 Euclid 算法的每一步,说明链中每对数的最大公约数相同的原因.

42.Fibonacci 数列 1,1,2,3,5,8,13,…(每一项是前面两项之和)的相邻两项能否有大于 1 的最大公约数?

素因数分解的唯一性

43.异于 1 的正整数 p,如果它的正因数只有 1 和 p,则称为素数.若 p 是素数,n是正整数,那么 gcd (p,n)等于什么?

44.因为从 $p \mid a$ 可以得到 $p \leqslant a$,所以2 是素数.因为 3 不是 2 的倍数,所以 3 是素数.因为 5 不是 2,3 或 4 的倍数,所以 5 是素数.列出小于 30 的素数.

45. 在下面的表中 (如果你喜欢,可以用描图纸),删去 2 的所有倍 (保留 2);删去 3 的所有倍数 (保留 3);删去 5 的所有倍数 (保留 5);删去 7 的所有倍数(保留 7).

剩下的那些数是否全是素数?

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

46. 证明 1 与 101 之间的任何一个非素数必以 2, 3, 5 或 7 作为它的因数. 假定 $a=bc$, 其中 b 和 c 都不等于 1, 并分别考察 $b=c$ 和 $b<c$ 两种情形.

47. 问题 45 中所用的方法称为 Eratosthenes 筛法. 用这个方法确定 1000 以内的全体素数必需用到哪些素数?

48. 数 3, 5, 7, 11 都是素数, 而且 $5\cdot 7-3\cdot 11=2$. 再找四个素数 p, q, r, s, 使得 $pq-rs=2$. 能否找到四个素数 p, q, r, s, 使得 $pq-rs=1$? 你是否以为能找到四个不同的素数 p, q, r, s, 使得 $pq-rs=0$?

49. 为什么两个偶数的乘积必定是偶数? 表 1.4 中的数全是偶数. 从表中删去是偶数之积的那些数. 余下的数, 在某种意义上, 在这个集合中是"素"的. 按此约定, 明确地指出哪些数是"素数", 哪些数不是. 用两种不同的方式将 180 表示为"素数"之积. 找出另外的偶数, 它可以用两种不同的方式表示为"素数"之积.

50. 两个形如 $4n+1$ 的数之积为什么必定还是这种形式的

表 1.4

2	4	6	8				
10	12	14	16	106	108	110	112
18	20	22	24	114	116	118	120
26	28	30	32	122	124	126	128
34	36	38	40	130	132	134	136
42	44	46	48	138	140	142	144
50	52	54	56	146	148	150	152
58	60	62	64	154	156	158	160
66	68	70	72	162	164	166	168
74	76	78	80	170	172	174	176
82	84	86	88	178	180	182	184
90	92	92	96	186	188	190	192
98	100	102	104	194	196	198	200

数?

表 1.5 中的数都是 $4n+1$ 的形式. 把凡是表中(不等于 1)的数的乘积的那些数都删去.余下的不等于 1 的那些数,在某种意义上,在这个集合中是"素"的.按此约定,在不超过 101 的数中,明确地指出哪些是"素数",哪些不是.将 441 用两种不同的方式表为"素数"之积.在表 1.5 中找出另一个数,它可以用两种不同方式表为"素数"之积.

51. 在普通算术中,我们假定,如果素数 p 整除乘积 ab,那么它必整除其中的一个因数,在各自约定了"素数"的偶数集合以及形如 $4n+1$ 的数集中,上述假定是否正确?

52. 设 p, q 和 r 都是素数而且 $p \neq q$,那么 gcd (p,q) 等于什么? 形如 $px+qy$ (x 与 y 是整数)的最小正整数等于什么? 形如 $rpx+rqy$ 的最小正整数等于什么? 此外,如果 $p \mid rq$,证明 $p \mid r$,从

而推出$p=r$.

表1.5

1	5	9	13	17	21	25	29	33	37
41	45	49	53	57	61	65	69	73	77
81	85	89	93	97	101	105	109	113	117
121	125	129	133	137	141	145	149	153	157
161	165	169	173	177	181	185	189	193	197
201	205	209	213	217	221	225	229	233	237
241	245	249	253	257	261	265	269	273	277
281	285	289	293	297	301	305	309	313	317
321	325	329	333	337	341	345	349	353	357
361	365	369	373	377	381	385	389	393	397
401	405	409	413	417	421	425	429	433	437
441	445	449	453	457	461	465	469	473	477
481	485	489	493	497	501	505	509	513	517
521	525	529	533	537	541	545	549	553	557
561	565	569	573	577	581	585	589	593	597
601	605	609	613	617	621	625	629	633	637
641	645	649	653	657	661	665	669	673	677
681	685	689	693	697	701	705	709	713	717
721	725	729	733	737	741	745	749	753	757
761	765	769	773	777	781	785	789	793	797
801	805	809	813	817	821	825	829	833	837
841	845	849	853	857	861	865	869	873	877
881	885	889	893	897	901	905	909	913	917
921	925	929	933	937	941	945	949	953	957
961	965	969	973	977	981	985	989	993	997

53. 利用上题结果,证明不可能找到四个不同的素数p,q,r s,使得$ps-qr=0$.

54. 推广52题中的论证,证明:如果p是素数,a和b是非零整数,而且$p|ab$,则$p|a$或者$p|b$(假设p不能整除a).

55. 利用上题结果证明,不可能找到五个不同的素数p,q,r, s及t,使得$pq=rst$.事实上,不可能找到五个素数(不论是否相同)满足这个方程.

56. 设p,q,r,s是素数,证明由$p\mid qr$可以推出$p=q$或$p=r$,而且由$p\mid qrs$可以推出$p=q$或$p=r$或$p=s$.

57. 设$p_1,\cdots,p_n$以及$q_1,\cdots,q_m$都是素数(但不必全不相同).而且

$$p_1\cdots p_n=q_1\cdots q_m.$$

证明p_1至少与某个q_1相等.对上等式除以这个因数后,证明p_2等于另一个q_1.对因子个数使用归纳法,证明$n=m$,而且每个p_1与一个q_1相等.

将5247000表示为素数之积.

58.设$p_1,\cdots,p_n$是正整数a(>1)的所有不同的素因数,证明

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n},$$

其中α_1是唯一确定的正整数.

(算术基本定理)

59.利用5247000和189280的素因数分解式,求它们的gcd和lcm.

如果允许指数为零,写出两个数的最大公约数与最小公倍数的公式.

证明两数之积等于它们的gcd与lcm之积.

60.若gcd $(a,b)=1$,则称a与b互素.设gcd $(a,b)=1$及gcd $(a,c)=1$,证明gcd $(a,bc)=1$.

61.若a与b互素而且$a|bc$,则$a\mid c$.

素数的无限性

62.数$2\cdot3\cdot5\cdot7\cdot11\cdot13+1$不是素数.关于它的素因数你能说些什么?

63.若p与q是任意两个素数,关于$pq+1$的素因数你能说些什么?

64.假定将素数依照大小排列:$p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$, $p_5=11$,等等.又假定

$$p_m|p_1p_2\cdots p_n+1.$$

关于m你能说些什么?

证明全体素数的个数不能是有限的，而且

$$p_{n+1} \leqslant p_1 p_2 \cdots p_n + 1 .$$

65．设 a 是正整数，证明 $4a-1$ 的素因数都是奇数．

表 1.1 中哪些列含有素数?

若四个奇素数之积在表1.1 的右边那一列，那么它们之中有几个一定的在这一列？

若 n 个奇素数之积与 3 对模 4 同余，那么，它们之中有几个一定与 3 对模 4 同余?

对于

$$4p_2 p_3 \cdots p_n - 1$$

的素因数你能说些什么？

证明：与 3 对模 4 同余的素数的个数是无限的．

66．考察形如 $3a-1$ 的数的因数并证明：与 2 对模 3 同余的素数的个数是无限的．

Mersenne 素 数

67．利用计逢器，写出当 $n=1,2,\cdots,16$ 时的 2^n-1 的值．

设 $2^n-1=m$，你能为命题

“若 n 是素数，则 m 是素数”

或者

“若 m 是素数，则 n 是素数”

提出证据吗？

(当 m 是素数时，称它为 Mersenne 素数)．

注记与答案

预备读物见参考书目，特别是 Reid (1956)，Ore (1967) 及

Butts (1973). 本章参考书还可用 Davenport (1968).

1. 数论主要研究自然数

$$N=\{1,2,3,\cdots\}$$

的性质. 但是,最好是在更广的范围内考察这些数,例如:整数集合

$$Z=\{0,\pm 1,\pm 2,\pm 3,\cdots\},$$

有理数集合

$$Q=\{\frac{p}{q}\mid p,q\in Z,q\neq 0\},$$

与直线上的所有点对应的实数集合R,或者复数集合

$$C=\{x+iy\mid x,y\in R,i^2=-1\}.$$

2. 少4,或者说多4.

3. 4的倍数.

4. $4n+4m=4(n+m)$.

5. $4n+1$, $4n+2$, $4n+3$.

6. 在第一列, $(4n+1)-(4m+1)=4(n-m)$.

7. $(4n+2)-(4m+2)=4(n-m)$.

8. $(4n+3)-(4m+3)=4(n-m)$.

9. 在第三列, $(4n+1)+(4m+1)=4(n+m)+2$.

10. 在第三列, $(4n+3)+(4m+3)=4(n+m+1)+2$.

11.

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

12. $a-b$ 有因数4.

13. $4\,\underline{|\,1553}$

$\quad 388$ 余1,

于是 $1553=4\cdot 388+1$.

14.

0	0	0	0
0	1	2	3
0	2	0	2
0	3	2	1

例如 $(4n+2)(4m+2)=4(4mn+2m+2n+1)$.

15 . $5n$,$5n+1$,$5n+2$,$5n+3$, $5n+4$.

16 . 5 | 6 6 6 6

1 3 3 3 余 1 ,

于是 $6666=5 \cdot 1333+1$.

17 . 加法 乘法

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	0	0	0	0
0	1	2	3	4
0	2	4	1	3
0	3	1	4	2
0	4	3	2	1

$(5n+2)+(5m+3)=5(n+m+1)$.

$(5n+2)+(5m+4)=5(5mn+2m+4n+1)+3$.

18 . 第一行 $0,1,2,\cdots,b-1$.

第一列 $0, b, b\cdot 2, b\cdot 3, \cdots$.

$bq\leqslant a<b(q+1)$, 于是$0\leqslant a-bq<b$ 而且 $0\leqslant r<b$.

自然数的一个基本性质是 : 重复地加 1 就可以大于任何给定的数 . 此处的论据基本假设 : 重复加 b 就可以大于 a . $b(q+1)$ 是第一个这样的倍数 .

字母 q 表示商 ,字母 r 表示 a 被 b 除后所得的余数 .

19 . $b(q_1-q_2)=r_2-r_1$,但是$0\leqslant r_1, r_2<b$, 所以 $-b<r_1-r_2<b$. 由于 r_2-r_1 是 b 的倍数 ,所以 $r_2-r_1=0$.

20 . $4n$, $4n+1$, $4n+2$, $4n+3$. 是 . 是 .

21．$-161=4(-41)+3$．

22．$4Z$ 是 $(Z,+)$的子群，而 $4Z+1$，$4Z+2$，$4Z+3$ 都是它的陪集．

23．给出任意的整数 a 和正整数 b，存在唯一的整数 q 与唯一的整数 r，满足 $0\leqslant r<b$，使得 $a=bq+r$．

24．选取 q，使得 $a-bq$ 是可能达到的最小正整数或零．于是 $a-b(q+1)<0\leqslant a-bq$，从而 $a-bq<b$ 而且 $0\leqslant r=a-bq<b$．唯一性的证明和问题 19 相同．

25．$\{170,130\}\to\{40,130\}\to\{40,90\}\to\{40,50\}\to\{40,10\}\to\{30,10\}\to\{20,10\}\to\{10,10\}=\{10\}$ 停止．

26．$\{a,b\}\to\{a-b,b\}$．若 $a>b>0$ 则 $b<0$ 而且 $a-b>0$．若 $a-b=0$，则$a=b$ 而且$\{a,b\}=\{a\}$．

27．$(1,0)$，$(0,1)$，$(1,-1)$，$(-1,2)$，$(2,-3)$，$(-3,5)$，$(-5,8)$．

28．$(0,1)$，$(1,0)$，$(-1,1)$$(2,-1)$，$(-3,2)$，$(-5,3)$，$(-7,4)$，$(9,-5)$．

29．由问题 27 知道 3 在这个集合中；$57x+36y=3(19x+12y)$．

30．3 的倍数．

31．由问题 28 知道 7 在这个集合中；$98x+175y=7(14x+25y)$．

32．7 的倍数．

33．$\{ax+by\mid x,y\in Z\}$．若$d=ax+by$，则 $nd=a(nx)+b(ny)$．若对任何 q，$c\neq dq$，则 $c=dq+r$，$0<r<d$．但是由于 c 属于这个子群，从而推出 $c-dq$ 也属于这个子群．

34．因为由 d 所生成的子群是由它的所有倍数组成的，所以 a 和 b 是 d 的倍数，即 $d\mid a$，$d\mid b$．因为 d 在由 a，b生成的子群中，所以 $d=ax+by$ (x,y 是某两个整数)．因此，a 与 b 的任一公因数整除 $ax+by$，从而整除 d．

如果以前你没有见过这个结论，你将会为 $\gcd(a,b)=ax+by$

(x ,y 是某两个整数)这一事实的作用而惊奇．我们要用它来证明素因数分解的唯一性,在本书许多章节中也将用到它．

35．gcd (2 ,3) = 1 ,因而存在整数 x 与 y,使得 $2x+3y=1$,例如 $2(-4)+3\cdot3=1$．

由 $2(a-c)=3(d-b)$推出 d－b 是偶数,于是 3 (d－b)＝$6t$.因此 $a=c+3t$,b＝$d-2t$．又因 $c=-4,d=3$ 是一组解,结论得证.

36．检验封闭性,单位元,逆远,$12x+18y+27z=3(4x+6y+9z)$. $12(-2)+18\cdot0+27\cdot1=3$．

37．如果 d 是集合$\{ax+by+cz\mid x,y,z\in Z\}$中的最小正整数,那么由注记 33 的论证知道,这个子群中的每个元素是 d 的倍数．因为这个子群是封闭的,所以它含有 d 的所有倍数．

38．使用注记 37 里的 d ,那里已经证明了 $d\mid a$, $d\mid b$, $d\mid c$,若 $d=ax+by+cz$,则 a ,b 与 c 的每个公约数整数 d．

39．若 $a<b$ 而且 a 不是 b 的倍数,则$\{a,b\}\to\{b,a-bq\}$,其中 $0<a-bq<b$．

40．1342．

41．

$57=36+21$,
$36=21+15$,
$21=15+6$,
$15=6\cdot2+3$,
$6=3\cdot2$.

$175=98+77$,
$98=77+21$,
$77=21\cdot3+14$,
$21=14+7$,
$14=7\cdot2$.

若 $a>b$ 而且 a 不是 b 的倍数,则$\{a,b\}\to(b ,a-bq\}$.

若 d ＝gcd (a ,b) ,则 $d\mid b$ 且 $d\mid a-bq$．

若 c＝gcd $(b ,a-bq)$, 则 $c\mid(a-bq)+bq=a$．

于是 $c\mid a$,$c\mid b$,从而 $c\mid d$．

42．若 $a_{n+1}=a_n+a_{n-1}$,则 a_{n+1} 与 a_n 的任何公因数也是 a_{n-1} 的因数．依此类推 ,可知任意一个这样的因数必是 Fibonacci 数列

中 a_n 前面所有项的因数.

43. $\gcd(p, n)=1$ 或 p.

44. 我们假定 a 是正数,2,3,5,7,11,13,17,19,23,29.

45. 是.

46. $10^2=100$,因此,若 $a=b^2<101$,则 $b\leqslant 10$,所以 b 有一个小于 10 的素因数,从而 a 也是如此.若 $a=bc<101$ 而且 $b>c$,这时 $b>c>10$ 是不可能的,所以 $c<10$,从而 c 和 a 都有小于 10 的素因数.

47. $31^2=961$, $32^2=1024$.只需要考虑不超过 31 的素数.若有机会,请编一个能打印出 1000 以内素数的计算机程序.

48. 素因数分解唯一性定理在学校的算术课本中被看做是当然成立的.本问题及下面两个问题试图说明对此给出一个证明的必要性.

$$3\cdot 19-5\cdot 11=2.$$
$$3\cdot 5-2\cdot 7=1.$$

49. 4 的倍数不是"素数".

形如 $4n+2$ 的数是"素数".

$$180=18\cdot 10=6\cdot 30$$
$$60=6\cdot 10=2\cdot 30$$

50. $(4m+1)(4n+1)=4(4mn+m+n)+1$.

5,9,13,17,21,29,33,37,41,49,53,57,61,69,73,77,89,93,97 是"素数".

$$441=21\cdot 21=9\cdot 49.$$
$$693=21\cdot 33=9\cdot 77.$$

51. 否.

52. 因为 $\gcd(p, q)=1$,所以存在整数 x, y,使得 $px+qy$ 1 以及 $rpx+rpy=r$.

由 $p \mid rq$ 推出 $p \mid rpx+rqy=r$. 但 r 是素数,所以 $p=r$.

53. 由 $ps=qr$ 推出 $p \mid qr$. 根据上题可知 $p=q$ 或 $p=r$.

54. 若 p 不整除 a,则 $\gcd(p, a)=1$. 因此存在整数 x, y,使得 $px+ay=1$, $bpx+bay=b$. 所以 $p \mid bpx+bay=b$.

55. 由 $pq=rst$ 推出 $p \mid rst$, 故由问题 54 可知 $p \mid r$ 或 $p \mid st$. 而由问题 52 可以 $p=r$ 或 $p=s$ 或 $p=t$. 若 $p=r$,则 $q=st$,这与 q 是素数相矛盾.

56. 根据问题 52 知,由 $p \mid qr$ 推出 $q=q$ 或 $p=r$.

按问题 54 知,由 $p \mid qrs$ 推出 $p \mid qr$ 或 $p \mid s$. 从而 $p=q$ 或 $p=r$ 或 $p=s$.

57. 因为 $p_1 \mid p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$,故由问题 54 知,$p_1 \mid q_1$ 或 $p_1 \mid p_2 \cdots q_m$.

若 $p_1 \neq q_1$,则 $p_1 \mid q_2$ 或 $p_1 \mid q_3 \cdots q_m$.

若 $p_1 \neq q_1$,则 $p_1 \mid q_3$ 或 $p_1 \mid q_4 \cdots q_m$,等等.

因此,$p_1=q_1$ 或 $p_1=q_2$ 或 $p_1=q_3 \cdots$ 或 $p_1=q_m$.

假定 $p_1=q_1$,则 $p_2 \cdots p_n = q_2 \cdots q_m$.

如果假定素因数分解式当因数为 $n-1$ 个时是唯一的,那么上面的论证表明当因数为 n 个时也是唯一的. 当 $n=1$ 时,素因数分解式显然是唯一的,所以由归纳法得证.

$$5247000 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 11 \cdot 53.$$

58. 设 $p_1 \mid a$, α_1 是使 $p_i^{\alpha_i} \mid a$ 的最大正整数,则 $p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_n^{\alpha_n} \mid a$. 于是 $a = kp_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$. 现在,$a$ 的素因数只有 $p_1, \cdots, p_n$,故由问题 57 知,k 的素因数也只能是 $p_1, \cdots, p_n$,但 α_1 是最大的,所以不可能再有 $p_i \mid k$,因而 $k=1$.

59. $189280 = 2^5 \cdot 5 \cdot 7 \cdot 13^2$,因此 $\gcd = 2^3 \cdot 5$,而且 $\mathrm{lcm} = 2^5 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13^2 \cdot 53$.

设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$,其中 $p_1, p_2, \cdots, p_n$ 包括了 a 和 b 的所有素因数,则

gcd $(a,b)=$ 所有的 $p_i^{\min(\alpha_i,\beta_i)}$之积.

lcm $(a,b)=$ 所有的 $p_i^{\max(\alpha_i,\beta_i)}$之积.

由于不管哪一个较大,都有 $\min\{\alpha,\beta\}+\max\{\alpha,\beta\}=\alpha+\beta$,所以

$$[\gcd(a,b)]\cdot[\operatorname{lcm}(a,b)]=ab$$

60. 由 gcd $(a,b)=1$ 可知,存在整数 x,y 使得 $ax+by=1$,从而 $cax+cby=c$. 若 gcd $(a,bc)=d$,则 $d\mid c$. 因为 gcd $(a,c)=1$,所以 $d=1$.

另法:考虑 a,b,c 的素因数.

61. 由 gcd $(a,b)=1$ 可知,存在整数 x,y 使得 $ax+by=1$,$acx+bcy=c$. 因此,由 $a\mid bc$ 推出 $a\mid c$.

62. 素因数不等于 2,3,5,7,11,13.

63. 素因数不等于 p,q.

64. $m\neq 1,2,\cdots,n$,所以 $m>n$.

这种构造方法,在任何有限素数的集合之外,又给出了一个素数. 因此,全体素数的集合是无限的.

存在一个大于 p_n 而且整除 $p_1\cdots p_n+1$ 的素数,所以 p_{n+1} 小于或等于这个素数,从而 $p_{n+1}\leqslant p_1\cdots p_n+1$.

65. 偶数 × 偶数 = 偶数.

偶数 × 奇数 = 偶数.

因此,2 不是奇数 $4a-1$ 的因数.

每个奇素数具有 $4n+1$ 或 $4n+3$ 的形式.

模 4

×	1	3
1	1	3
3	3	1

若四个奇素数之积为 $4n+3$,则其中一定有一个或者三个是 $4n+3$ 的形式. $4p_2p_3\cdots p_n-1$ 是奇数而且是 $4n+3$ 的形式,所以它有奇数个(因而至少有一个)形如 $4n+3$ 的素因数. 但这个数的所有素因数都比 p_n 大,所以对于给定的任何形如 $4n+3$

的素数,我们能构造出一个比它大而且有同样形式的素数.

66. $3a-1$ 与 2 对模 3 同余.

模 3 ×	1	2
1	1	2
2	2	1.

因此,$3a-1$ 必含有奇数个与 2 同余(mod3)的因数.但是 $2\cdot3\cdot p_3\cdot p_4\cdots p_{n-1}-1$ 不能被任何一个不超过 p_n 的素数整除,所以它的所有素因数都比 p_n 大.这样,对于给定的任何形如 3n+2 的素数,我们能构造一个比它大而且有同样形式的素数.

67. $2^{ab}-1=(2^a-1)(2^{a(b-1)}+2^{a(b-2)}+\cdots2^{a\cdot2}+2^a+1)$.

因此,若 m 是素数,则 n 也是素数. $2^{11}-1=23\cdot89$. 当 2^p-1 是素数时,$2^{p-1}(2^p-1)$的所有约数之和等于它自己的两倍.这一事实使 Mersenne 对这种数产生了兴趣.

历史注记

本章的所有定理,实质上都来自 Euclid(公元前 300 年);就除法算式以及求两个给定数的最大公约数的算法来说,显然是这样.Euclid 的记号妨碍了完善地叙述或证明算术基本定理和存在无限多个素数的论断.这些定理的实质性论证是属于 Euclid 的,尽管他只是讨论了至多三个或四个素数之积.C.F.Gauss(在 1801 年)第一次明确地叙述并证明了我们现在所知道的一般形式的基本定理,虽然,在他之前许多数学家就已经用了这个结论.1775 年,L.Euler 断言每个首项为 1 的算术级数含有无限多个素数.1837 年 Dirichlet 证明了:若 a 与 b 互素,则集合$\{an+b\,|\,n\in\mathrm{N}\}$含有无限多个素数.

第二章　模加法与 Euler 的 φ 函数

同余类与中国剩余定理[①]

1. 设 a,b 是表 2.1 中的数，并且 6 是 $a-b$ 的因数，那么关于 a 与 b 在表中的位置你能说些什么？

2. 若 6 是 $a-b$ 的因数，则记

$$a \equiv b \pmod{6},$$

我们说 a 同余于 b 模 6[②].

说明对于任何正整数 a 都有 $a \equiv a \pmod{6}$.

若 $a \equiv b \pmod{6}$，证明 $b \equiv a \pmod{6}$.

若 $a \equiv b \pmod{6}$ 并且 $b \equiv c \pmod{6}$，证明 $a \equiv c \pmod{6}$.

3. 确定同余于 0 $\pmod{6}$ 的所有整数的集合.
   确定同余于 1 $\pmod{6}$ 的所有整数的集合.
   确定同余于 2 $\pmod{6}$ 的所有整数的集合.
   确定同余于 3 $\pmod{6}$ 的所有整数的集合.
   确定同余于 4 $\pmod{6}$ 的所有整数的集合.
   确定同余于 5 $\pmod{6}$ 的所有整数的集合.

这六个集合称为模 6 的同余类或剩余类. 用除法算式证明每个整数恰好属于一个类.

4. 当 n 是 $a-b$ 的因数时，记

$$a \equiv b \pmod{n},$$

读作 a 同余于 b 模 n[③].

---

① 又称“孙子定理”。——译者注。

② 见问题 4 及其注。——译者注。

③ 也读作 a 与 b 对模 n 同余，记作 a 同余于 $b \pmod{n}$。——译者注。

此处我们约定 a 和 b 是整数，而且 n 是正整数.
叙述并证明问题 2 与问题 3 对模 n 的推广.

表 2.1

−90	−89	−88	−87	−86	−85
−84	−83	−82	−81	−80	−79
−78	−77	−76	−75	−74	−73
−72	−71	−70	−69	−68	−67
−66	−65	−64	−63	−62	−61
−60	−59	−58	−57	−56	−55
−54	−53	−52	−51	−50	−49
−48	−47	−46	−45	−44	−43
−42	−41	−40	−39	−38	−37
−36	−35	−34	−33	−32	−31
−30	−29	−28	−27	−26	−25
−24	−23	−22	−21	−20	−19
−18	−17	−16	−15	−14	−13
−12	−11	−10	−9	−8	−7
−6	−5	−4	−3	−2	−1
0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29
30	31	32	33	34	35
36	37	38	39	40	41
42	43	44	45	46	47
48	49	50	51	52	53
54	55	56	57	58	59
60	61	62	63	64	65
66	67	68	69	70	71
72	73	74	75	76	77
78	79	80	81	82	83
84	85	86	87	88	89
90	91	92	93	94	95

5. 用描图纸或复制下表，将数 0, 1, 2, 3, 4, 5 填入下面给出的阵列的适当的方格中. 例如 $4 \equiv 0 \pmod{2}$ 和 $4 \equiv 1 \pmod{3}$.

模 3

模2	0	1	2
0			
1			

6. 用描图纸或复制下表，将数0，1，2，…，9，10，11填入下面给出的阵列的适当的方格中.

模 4

模3	0	1	2	3
0				
1				
2				

7. 用描图纸或复制下表，将数0，1，2，…，33，34，35填入下面给出的阵列的适当的方格中.

模 9

模4	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									

8. $432=16\times 27$.

将数0，1，2，…，429，430，431 填入16×27的阵列中，使得每一列中的数两两对模 27 同余，每一行中的数两两对模 16 同余. 能否断定 0 与 431 之间没有两个整数会填入同一位置？每个方格中是否恰好有一个在 0 与 431 间的数？

9. 用描图纸或复制下表，将数0，1，2，…，9，10，11填入下面给出的阵列的适当方格中.

模6

		0	1	2	3	4	5
模2	0						
	1						

为什么类似于问题8中所用的推理在此处不适用？

10. 用描图纸或复制下表，将数0，1，2，…，57，58，59填入下面给出的阵列的适当方格中.

模10

		0	1	2	3	4	5	6	7	8	9
模6	0										
	1										
	2										
	3										
	4										
	5										

为什么问题8中所用的推理在此处不适用？

11. 假如你要推广问题8的论证来证明：在0与$mn-1$之间不存在两个不同的数，它们对模m和模n都同余. 那么，为了避免出现问题9和10中的情形，对m和n应加上什么条件？

12. 设a和b是整数，而且

$$a \equiv b \pmod{m}, \quad a \equiv b \pmod{n}.$$

证明：若m与n互素，则$a \equiv b \pmod{mn}$. 进而推出，若$0 \leqslant a$，$b \leqslant mn-1$，则$a=b$.

13. 当m和n互素时，为什么一定存在唯一的整数x，

$0 \leqslant x \leqslant mn-1$，使得

$x \equiv a_1 \pmod m$ 而且 $x \equiv a_2 \pmod n$?

14. 求 $x, 0 \leqslant x < 15$，使得 $x \equiv 2 \pmod 3$ 且 $x \equiv 4 \pmod 5$.

15. 求 $x, 0 \leqslant x < 120$，使得 $x \equiv 14 \pmod{15}$ 且 $x \equiv 5 \pmod 8$.

16. 求 $x, 0 \leqslant x < 120$，使得 $x \equiv 2 \pmod 3$，$x \equiv 5 \pmod 8$ 且 $x \equiv 4 \pmod 5$.

17. 推广问题 12 与 13 的论证来证明：若 m_1, m_2, m_3 两两互素，则

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$

存在唯一解 $\pmod{m_1 m_2 m_3}$①.

18. 用归纳法推广上题的论证. 证明：若 $m_1, m_2, \cdots, m_n$ 是两两互素的，则 n 个同余方程

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \cdots, n$$

存在唯一解 $\pmod{m_1 m_2 \cdots m_n}$①.

(中国剩余定理).

这个定理完成了对同余类的交集的研究. 在问题 50 中，将用中国剩余定理来证明 Euler $-\varphi$ 函数是积性函数. 现在，我们来考虑同余类的运算.

群 $(\mathbf{Z}_n, +)$ 及其生成元

19. 集合 $\{6n+1 \mid n \in \mathbf{Z}\}$ 与 $\{6n-5 \mid n \in \mathbf{Z}\}$ 是否相同?

20. 为什么每个整数恰好与整数 $-12, -5, 8, -3, -8, 23$ 中的一个对模 6 同余? 由于其中的每个数代表了模 6 的一个剩余

---

① 即若有 x_1 与 x_2 都满足这 n 个同余式，那么 $x_1 \equiv x_2 \pmod{m_1 m_2 \cdots m_n}$. ——译者注.

类，我们称这样的集合为模 6 的一个完全剩余系.

21. 设 $a_1, a_2, a_3, a_4, a_5, a_6$ 是整数，而且任何两个都不对模 6 同余，它们是否构成模 6 的一个完全剩余系?

22. 若 $a \equiv b \pmod{6}$ 而且 $c \equiv d \pmod{6}$，是否 $a+c \equiv b+d \pmod{6}$ 而且 $a-c \equiv b-d \pmod{6}$?

23. 用完全剩余系 0,1,2,3,4,5 做出模 6 的加法表 (见问题 1.11). 这是不是一个群表? 单位元是什么? 有没有一个元素，它生成这个群?

24. 用完全剩余系 12, −5, 8, −3, −8, 23 做出模 6 的加法表. 这个表的结构与上题中的表的结构是否一致? 单位元是什么? 有没有一个元素，它生成这个群?

25. 设 $\{a_1, a_2, a_3, a_4, a_5, a_6\}$ 是模 6 的任一完全剩余系，能否用这些元素来做一个群表，使得当 $a_i + a_j \equiv a_k \pmod{6}$ 时，a_k 是 a_i 与 a_j 的和? 完全剩余系上的这种加法，称为对模 6 的加法. 这个表与问题 23 中的表一定有同样的结构吗? 单位元是什么? 有生成元吗?

26. 设 $a \equiv b \pmod{n}$ 且 $c \equiv d \pmod{n}$，证明 $a+c \equiv b+d \pmod{n}$ 且 $a-c \equiv b-d \pmod{n}$.

27. 用表 2.2 中列出的群 $(\mathbf{Z}_3, +), \cdots, (\mathbf{Z}_{10}, +)$ 的例子，在对模 3, 4, 5, 6, 7, 8, 9, 10 的加法下，分别确定以下各个数列

$$1, 1+1, 1+1+1, \cdots$$
$$2, 2+2, 2+2+2, \cdots$$
$$3, 3+3, 3+3+3, \cdots$$

中的前十项.

28. 数列 $1, 1+1, 1+1+1, \cdots$ 是否包含任意模的所有剩余类? 为什么?

29. 数列 $2, 2+2, 2+2+2, \cdots$ 是否包含任意模的所有剩余类? 剩余类全被这个数列所包含的模有没有一个表示式? 剩余类不全被这个数列所包含的模有没有一个表示式? 能否给出证明?

30. 数列 $3, 3+3, 3+3+3, \cdots$ 是否包含任意模的所有剩余类？剩余类全被这个数列所包含的模，有没有一般的表示式？剩余类不全被这个数列所包含的模有没有一般的表示式？能否给出证明？

31. 在模 $n=7,8,\cdots,16$ 中，哪一个模的剩余类都包含在数列 $6, 6+6, 6+6+6, \cdots$ 中？

表 2.2

模 3 加法

0	1	2
1	2	0
2	0	1

模 4 加法

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

模 5 加法

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

模 6 加法

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

模 7 加法

0	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

模 8 加法

0	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
4	5	6	7	0	1	2	3
5	6	7	0	1	2	3	4
6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

模 9加法

0	1	2	3	4	5	6	7	8
1	2	3	4	5	6	7	8	0
2	3	4	5	6	7	8	0	1
3	4	5	6	7	8	0	1	2
4	5	6	7	8	0	1	2	3
5	6	7	8	0	1	2	3	4
6	7	8	0	1	2	3	4	5
7	8	0	1	2	3	4	5	6
8	0	1	2	3	4	5	6	7

模 10 加法

0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	0
2	3	4	5	6	7	8	9	0	1
3	4	5	6	7	8	9	0	1	2
4	5	6	7	8	9	0	1	2	3
5	6	7	8	9	0	1	2	3	4
6	7	8	9	0	1	2	3	4	5
7	8	9	0	1	2	3	4	5	6
8	9	0	1	2	3	4	5	6	7
9	0	1	2	3	4	5	6	7	8

模 11 加法

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
9	10	0	1	2	3	4	5	6	7	8
10	0	1	2	3	4	5	6	7	8	9

模 12 加法

0	1	2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6	7	8	9	10	11	0
2	3	4	5	6	7	8	9	10	11	0	1
3	4	5	6	7	8	9	10	11	0	1	2
4	5	6	7	8	9	10	11	0	1	2	3
5	6	7	8	9	10	11	0	1	2	3	4
6	7	8	9	10	11	0	1	2	3	4	5
7	8	9	10	11	0	1	2	3	4	5	6
8	9	10	11	0	1	2	3	4	5	6	7
9	10	11	0	1	2	3	4	5	6	7	8
10	11	0	1	2	3	4	5	6	7	8	9
11	0	1	2	3	4	5	6	7	8	9	10

模 13 加法

0	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	0
2	3	4	5	6	7	8	9	10	11	12	0	1
3	4	5	6	7	8	9	10	11	12	0	1	2
4	5	6	7	8	9	10	11	12	0	1	2	3
5	6	7	8	9	10	11	12	0	1	2	3	4
6	7	8	9	10	11	12	0	1	2	3	4	5
7	8	9	10	11	12	0	1	2	3	4	5	6
8	9	10	11	12	0	1	2	3	4	5	6	7
9	10	11	12	0	1	2	3	4	5	6	7	8
10	11	12	0	1	2	3	4	5	6	7	8	9
11	12	0	1	2	3	4	5	6	7	8	9	10
12	0	1	2	3	4	5	6	7	8	9	10	11

模 14 加法

0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	2	3	4	5	6	7	8	9	10	11	12	13	0
2	3	4	5	6	7	8	9	10	11	12	13	0	1
3	4	5	6	7	8	9	10	11	12	13	0	1	2
4	5	6	7	8	9	10	11	12	13	0	1	2	3
5	6	7	8	9	10	11	12	13	0	1	2	3	4
6	7	8	9	10	11	12	13	0	1	2	3	4	5
7	8	9	10	11	12	13	0	1	2	3	4	5	6
8	9	10	11	12	13	0	1	2	3	4	5	6	7
9	10	11	12	13	0	1	2	3	4	5	6	7	8
10	11	12	13	0	1	2	3	4	5	6	7	8	9
11	12	13	0	1	2	3	4	5	6	7	8	9	10
12	13	0	1	2	3	4	5	6	7	8	9	10	11
13	0	1	2	3	4	5	6	7	8	9	10	11	12

模 15 加法

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
2	3	4	5	6	7	8	9	10	11	12	13	14	0	1
3	4	5	6	7	8	9	10	11	12	13	14	0	1	2
4	5	6	7	8	9	10	11	12	13	14	0	1	2	3
5	6	7	8	9	10	11	12	13	14	0	1	2	3	4
6	7	8	9	10	11	12	13	14	0	1	2	3	4	5
7	8	9	10	11	12	13	14	0	1	2	3	4	5	6
8	9	10	11	12	13	14	0	1	2	3	4	5	6	7
9	10	11	12	13	14	0	1	2	3	4	5	6	7	8
10	11	12	13	14	0	1	2	3	4	5	6	7	8	9
11	12	13	14	0	1	2	3	4	5	6	7	8	9	10
12	13	14	0	1	2	3	4	5	6	7	8	9	10	11
13	14	0	1	2	3	4	5	6	7	8	9	10	11	12
14	0	1	2	3	4	5	6	7	8	9	10	11	12	13

模 16 加法

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	0
2	3	4	5	6	7	8	9	10	11	12	13	14	15	0	1
3	4	5	6	7	8	9	10	11	12	13	14	15	0	1	2
4	5	6	7	8	9	10	11	12	13	14	15	0	1	2	3
5	6	7	8	9	10	11	12	13	14	15	0	1	2	3	4
6	7	8	9	10	11	12	13	14	15	0	1	2	3	4	5
7	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6
8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	10	11	12	13	14	15	0	1	2	3	4	5	6	7	8
10	11	12	13	14	15	0	1	2	3	4	5	6	7	8	9
11	12	13	14	15	0	1	2	3	4	5	6	7	8	9	10
12	13	14	15	0	1	2	3	4	5	6	7	8	9	10	11
13	14	15	0	1	2	3	4	5	6	7	8	9	10	11	12
14	15	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

32. 如果数列 $a, a+a, a+a+a, \cdots$ 包含 $\mathbf{Z}_n$ 的所有元素，则称 a 是群 $(\mathbf{Z}_n,+)$ 的生成元. 举出 $(\mathbf{Z}_2,+)$, $(\mathbf{Z}_4,+)$, $(\mathbf{Z}_8,+)$ 及 $(\mathbf{Z}_{16},+)$ 的生成元.

说明为什么这些群中任何一个的生成元都不是偶数.

试猜测 $(\mathbf{Z}_{2^k},+)$ 的生成元的个数.

33. 举出 $(\mathbf{Z}_3,+)$, $(\mathbf{Z}_9,+)$, $(\mathbf{Z}_{27},+)$ 的生成元.

说明为什么 3 的倍数不是这些群中任何一个的生成元.

试猜测 $(\mathbf{Z}_{3^k},+)$的生成元的个数.

34. 对模 n 考察数列 $a, a+a, a+a+a, \cdots$. 你能不能断定在 n 项之后这个数列就重复了?

35. 你在问题 27 中写下的每个数列中，第一个重复的数是什么?

36. 假设在数列

$$a, 2a, 3a, \cdots \quad \bmod n$$

中，在 $na+a$ 之前出现了重复. 特别地，设第一个重复出现在项 ka, 它与前面的项 la 重复，即 $ka \equiv la \pmod n$, $1 \leqslant l < k$. 证明在第 $k-l+1$ 项一定已经出现了重复，所以 $l=1$.

37. 假设在数列

$$a, 2a, 3a, \cdots \quad \bmod n$$

中的第一次重复是 $ka \equiv a \pmod n$, $1<k<n$, 证明 a 和 n 必定有一个公共的素因数.

38. 设 $\gcd(a,n) \neq 1$, 证明a 不是 $(\mathbf{Z}_n,+)$的生成元.

设 $\gcd(a,n)=1$, 证明数列

$$a, 2a, 3a, \cdots \quad \bmod n$$

在第 $n+1$ 项之前无重复，从而推出 a 是 $(\mathbf{Z}_n,+)$的生成元.

Euler 的 φ 函数

39. Euler 函数 $\varphi(n)$表示$(\mathbf{Z}_n,+)$的生成元的数目，或等价地，表示不超过 n 并且与 n 互素的正整数的个数. 写出当 $n=1, 2, \cdots, 10$ 时的 $\varphi(n)$的值.

40. 利用表 2.3 写出

$\varphi(2)$, $\varphi(4)$, $\varphi(8)$, $\varphi(16)$, $\varphi(32)$, $\varphi(64)$, $\varphi(128)$, $\varphi(256)$ 的值.

确定 $\varphi(2^n)$的值.

41. 利用表 2.4 写出

$\varphi(3)$，$\varphi(9)$，$\varphi(27)$，$\varphi(81)$，$\varphi(243)$的值.

确定 $\varphi(3^n)$的值.

表 2.3

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88
89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128

表 2.4

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99
100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117
118	119	120	121	122	123	124	125	126
127	128	129	130	131	132	133	134	135
136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153
154	155	156	157	158	159	160	161	162
163	164	165	166	167	168	169	170	171
172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189
190	191	192	193	194	195	196	197	198
199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216
217	218	219	220	221	222	223	224	225
226	227	228	229	230	231	232	233	234
235	236	237	238	239	240	241	242	243

表　2.5

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30
31	32	33	34	35
36	37	38	39	40
41	42	43	44	45
46	47	48	49	50
51	52	53	54	55
56	57	58	59	60
61	62	63	64	65
66	67	68	69	70
71	72	73	74	75
76	77	78	79	80
81	82	83	84	85
86	87	88	89	90
91	92	93	94	95
96	97	98	99	100
101	102	103	104	105
106	107	108	109	110
111	112	113	114	115
116	117	118	119	120
121	122	123	124	125

42. 利用表 2.5 写出

$\varphi(5)$，$\varphi(25)$，$\varphi(125)$的值.

确定 $\varphi(5^n)$的值.

43. 对于任意素数p，试述 $\varphi(p^n)$的值，并给出证明.

44. 求 $\varphi(2)\varphi(6)$与 $\varphi(3)\varphi(4)$. 哪一个等于 $\varphi(12)$?

45. 求 $\varphi(2)\varphi(9)$与 $\varphi(3)\varphi(6)$. 哪一个等于 $\varphi(18)$?

46. 证明: 一般来说，$\varphi(ab)\neq\varphi(a)\varphi(b)$. 对使 $\varphi(ab)=\varphi(a)\varphi(b)$的数 a 和 b 做一个猜测.

47. 问题 6 中所求的表是

		模 4			
		0	1	2	3
模 3	0	0	9	6	3
	1	4	1	10	7
	2	8	5	2	11

以 3 为因数的数在什么位置?

以 2 为因数的数在什么位置?

不与 12 互素的数是否一定有因数 2 或 3?

从表中删去以 2 或 3 为因数的数.

未被完全删去的行有 多少?

未被完全删去的列有多少?

这些行数和列数与 $\varphi(12)$有什么关系?

48. 利用下表，通过删去适当的行和列，说明

$$\varphi(36)=\varphi(4)\varphi(9).$$

模 9

		0	1	2	3	4	5	6	7	8
模4	0	0	28	20	12	4	32	24	16	8
	1	9	1	29	21	13	5	33	25	17
	2	18	10	2	30	22	14	6	34	26
	3	27	19	11	3	31	23	15	7	35

49. 如果一个整数不与 $432=16\cdot 27$ 互素，它是否一定有因数 2 或 3，或两者都有?

如果一个整数不与 432 互素，证明它与 0, 2, 4, 6, 8, 10, 12 或 14 中的一个对模 16 同余，或者与 0, 3, 6, 9, 12, 15, 18, 21 或 24 中的 一个对模 27 同余.

推导 $\varphi(16\cdot 27)=\varphi(16)\varphi(27)$.

50. 设 m 与 n 互素，证明任何一个与 mn 不互素的数一定与 m有素公因数，或与 n 有素公因数，或是二者兼有. 若将 mn 个数 $0, 1, 2, \cdots, mn-1$ 填到 $m\times n$ 长方阵列中，它的行是由对模 m 同余的数组成，它的列是由对模 n 同余的数组成，然后删去所有不与 mn 互素的数，证明任何一个被删去的数所在的行和列中，必有一个被完全删去,或二者都被完全删去. 由此推出 $\varphi(mn)=\varphi(m)\varphi(n)$. 这就是“$\varphi$ 为积性函数”的含义.

51. 利用上题证明：$\varphi(2^a3^b5^c)=\varphi(2^a)\varphi(3^b)\varphi(5^c)$.

52. 用归纳法证明：若$p_1, p_2, \cdots, p_n$是不同的素数，则

$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n})=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_n^{\alpha_n}).$$

53. 利用问题 43 证明

$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n})=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_n}).$$

54. 求$\varphi(60)$的另一个方法是考察由从 1 到 60 的数所组成的集合，并且只去数这个集合中的元素，于是

$$\begin{aligned}\varphi(60)=60-&(\text{以 2, 3 或 5 为因数的数的个数})\\ =60-&(\text{以 2 为因数的数的个数})\\ -&(\text{以 3 为因数的数的个数})\\ -&(\text{以 5 为因数的数的个数})\\ +&(\text{以 2 和 3 为因数的数的个数})\\ +&(\text{以 2 和 5 为因数的数的个数})\\ +&(\text{以 3 和 5 为因数的数的个数})\\ -&(\text{以 2, 3 和 5 为因数的数的个数}).\end{aligned}$$

求出括号中的数值并验证$\varphi(60)=\varphi(4)\varphi(3)\varphi(5)$.

55. 推广上题并证明：若p, q, r是不同的素数，则

$$\varphi(p^aq^br^c)=p^aq^br^c(1-\frac{1}{p}-\frac{1}{q}-\frac{1}{r}+\frac{1}{qr}+\frac{1}{rp}+\frac{1}{pq}-\frac{1}{pqr}).$$

由此及问题 43，证明

$$\varphi(p^aq^br^c)=\varphi(p^a)\varphi(q^b)\varphi(r^c).$$

56. 推广上题的论证，对于有四个不同素因数的数，计算 Euler 的φ函数值.

Euler 函数对约数求和

57. 6 的因数是 1, 2, 3, 6. 求

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6).$$

8 的因数是 1, 2, 4, 8. 求

$$\varphi(1)+\varphi(2)+\varphi(4)+\varphi(8).$$

12的因数是1, 2, 3, 4, 6, 12. 求

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12).$$

将这些结果写成下面的形式:

$$\sum_{d|6}\varphi(d)= \qquad , \quad \sum_{d|8}\varphi(d)= \qquad , \quad \sum_{d|12}\varphi(d)= \qquad .$$

58. 把从1到12的数排成一行.

凡是与12互素的数, 在它下面划条线. 这种数共有 $\varphi(12)=4$个. 把没有划过线的数再写在第一行下面.

在第二行中,凡是被2整除并且商与 $\frac{12}{2}=6$ 互素的数, 在它下面划条线. 这种数共有 $\varphi(6)=2$ 个. 把没有划过线的数再写在第二行下面.

第三行中,在凡是被3整除并且商与$\frac{12}{3}=4$互素的数的下面划线. 这种数共有 $\varphi(4)=2$ 个. 把没有划过线的数再写在第三行下面.

第四行中,在凡是被4整除并且商与$\frac{12}{4}=3$互素的数的下面划线. 这种数共有 $\varphi(3)=2$ 个. 把没有划过线的数再写在第四行下面.

第五行中,在被6整除并且商与$\frac{12}{6}=2$互素的数的下面划线. 这种数有 $\varphi(2)=1$ 个. 现在, 只有被12整除的数没有被划过线, 这样的数恰好有一个.

试刻画每一行中被划过线的数的特征.

59. 如果把数 $1, 2, \cdots, n$ 排成一行,并且按上题的方式来划线. 假定 n 的约数按递增顺序排列是 $1=d_1, d_2, \cdots, d_k=n$, 以及 $\gcd(a, n)=d_i$. 试问数 a $(1\leqslant a\leqslant n)$将在哪一行被划线? 与数 a 在同一行的数当中, 有多少个被划线?

60. 证明 $\sum\limits_{d|n}\varphi(d)=\sum\limits_{d|n}\varphi\left(\frac{n}{d}\right)$.

61. 定义$f(n)=\sum\limits_{d|n}\varphi(d)$, 利用问题43证明: 对于任意的素

数p，$f(p^\alpha)=p^\alpha$.

62. 只利用f的定义和当m,n互素时$\varphi(m)\varphi(n)=\varphi(mn)$这一事实，证明$f(9)f(8)=f(72)$. 由此推出$f(72)=72$.

63. 设m和n互素，说明下面每一步骤的合理性：

$$f(m)f(n)=\sum_{d|m}\varphi(d)\cdot\sum_{d'|n}\varphi(d')$$

$$=\sum_{d|m,d'|n}\varphi(d)\varphi(d')=\sum_{d|m,d'|n}\varphi(dd')$$

$$=\sum_{dd'|mn}\varphi(dd')=f(mn).$$

64. 利用问题61和上题证明：对于所有的正整数n，$f(n)=n$. 这个结果是证明素数模的原根存在性的关键步骤（问题3.61）.

注记与答案

参考书见书目：Davenport (1968)，Ore (1948)，Weil (1979).

1. a与b在同一列.

2. 因为$a-a=0=6\cdot 0$，所以$a\equiv b \pmod 6$

$$a\equiv b \pmod 6 \Rightarrow a-b=6k\Rightarrow b-a=6(-k)$$

$$\Rightarrow b\equiv a \pmod 6.$$

$$a\equiv b \pmod 6 \text{与} b\equiv c \pmod 6$$

$$\Rightarrow a-b=6k \text{与} b-c=6m$$

$$\Rightarrow a-c=6(k+m)\Rightarrow a\equiv c \pmod 6.$$

3. 若$a=6q+r$，$0\leqslant r<6$，则$a\equiv r \pmod 6$.

4. 在问题2中用n代替6.

5.

0	4	2
3	1	5

6.

0	9	6	3
4	1	10	7
8	5	2	11

7.

0	28	20	12	4	32	24	16	8
9	1	29	21	13	5	33	25	17
18	10	2	30	22	14	6	34	26
27	19	11	3	31	23	15	7	35

8. 若 a 和 b 在同一个位置，则 $a \equiv b \pmod{16}$ 而且 $a \equiv b \pmod{27}$，因而 $a-b=16n$，而且 $a-b=27m$. 于是 $a-b=16 \cdot 27k$，即 $a \equiv b \pmod{432}$. 因此每个位置上至多有一个数. 但是，432 个数共有 432 个位置，所以是一一对应的.

9.

0	6	–	2	8	–	4	10	–
–	1	7	–	3	9	–	5	11

6 和 2 有公因数，所以，由 $a \equiv b \pmod{6}$ 与 $a \equiv b \pmod{2}$ 仅能推出 $a \equiv b \pmod{6}$，而不是 $a \equiv b \pmod{12}$.

10.

0	30	–	12	42	–	24	54	–	6	36	–	18	48	–
–	1	31	–	13	43	–	25	55	–	7	37	–	19	49
20	50	–	2	32	–	14	44	–	26	56	–	8	38	–
–	21	51	–	3	33	–	15	45	–	27	57	–	9	39
10	40	–	22	52	–	4	34	–	16	46	–	28	58	–
–	11	41	–	23	53	–	5	35	–	17	47	–	29	59

10 和 6 有公因数，所以由 $a \equiv b \pmod{10}$ 与 $a \equiv b \pmod{6}$ 仅能推出 $a \equiv b \pmod{30}$，而不是 $a \equiv b \pmod{60}$.

11. m 与 n 互素.

12. $$\left.\begin{array}{l} a \equiv b \pmod{m} \Rightarrow a-b=mk \\ a \equiv b \pmod{n} \Rightarrow a-b=nh \end{array}\right\} \Rightarrow n \mid mk \text{，因而}$$

由注记 1.61 知 $n \mid k \Rightarrow a-b=mnl$

$$\Rightarrow a \equiv b \pmod{mn}.$$

13. 由问题 12 知道，不能有两个解．因此对于数对 (a_1, a_2) 的 mn 个取法中的每一个，在 mn 个数 $0, 1, 2, \cdots, mn-1$ 中都恰好有一个数与它对应．

14. 14.

15. 29.

16. 29.

17. 由问题 13 知道，

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2}$$

存在唯一解 $x=b$，$0 \leqslant b \leqslant m_1 m_2 - 1$．利用问题 1.60 及问题 13，又可证明

$$x \equiv b \pmod{m_1 m_2},$$
$$x \equiv a_3 \pmod{m_3}$$

存在唯一解 x，$0 \leqslant x \leqslant m_1 m_2 m_3 - 1$．

18. 假设对 $n-1$ 个这样的方程有唯一解，即存在唯一的 $x=b$，$0 \leqslant b \leqslant m_1 m_2 \cdots m_{n-1} - 1$，满足

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_{n-1} \pmod{m_{n-1}},$$

则由问题1.60 和问题 13 知道，存在唯一的 x，$0 \leqslant x \leqslant m_1 m_2 \cdots m_{n-1}$，满足

$$x \equiv b \pmod{m_1 m_2 \cdots m_{n-1}}$$

与

$$x \equiv a_n \pmod{m_n}.$$

由归纳法得出结论．

19. 是.

20. $-12\equiv 0 \pmod 6$, $-5\equiv 1 \pmod 6$, $8\equiv 2 \pmod 6$,

$-3\equiv 3 \pmod 6$, $-8\equiv 4 \pmod 6$, $23\equiv 5 \pmod 6$.

$\{6n+8 \mid n\in \mathbf{Z}\}=\{6n+2 \mid n\in \mathbf{Z}\}$, 等等.

21. 每个数与 0,1,2,3,4,5 中之一同余. 不可能有两个数同余于同一个数, 否则, 由问题 2 知, 这两个数将互为同余. 因此, 每个数恰好取自一个剩余类.

22. $a\equiv b \pmod 6 \Rightarrow a-b=6k$,

$c\equiv d \pmod 6 \Rightarrow c-d=6m$,

$(a+c)-(b+d)=6(k+m) \Rightarrow a+c\equiv b+d \pmod 6$,

$(a-c)-(b-d)=6(k-m) \Rightarrow a-c\equiv b-d \pmod 6$.

23.

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

0 是单位元. 1 生成这个群, 5 也生成这个群.

24.

12	−5	8	−3	−8	23
−5	8	−3	−8	23	12
8	−3	−8	23	12	−5
−3	−8	23	12	−5	8
−8	23	12	−5	8	−3
23	12	−5	8	−3	−8

12 是单位元. −5 生成这个群, 23 也生成这个群.

25. $a_1, \cdots, a_6$ 以某个顺序与 0, 1, 2, 3, 4, 5 对模 6 同余. 设 $a_i\equiv i \pmod 6$, 则 $a_i+a_j\equiv i+j \pmod 6$, 因而这个表与问题

23中的表构造相同．单位元是 $a_i \equiv 0 \pmod 6$，生成元是 $a_i \equiv 1 \pmod 6$．

这样得到的每个群都是群 $(\mathbf{Z}_6, +)$的一个例子，群 $(\mathbf{Z}_6, +)$ 可以定义为具有对模 6 加法的一个完全剩余系，也可以定义为以模 6 的剩余类为元素的集合，并且具有在问题 22 中所建立的那种由通常的整数加法引伸出的剩余类加法．这两种描述提供了相同的代数结构．

26．在问题 22 中用 n 代替 6．

27．见问题 28 — 30．

28．

mod 3	1	2	0	1	2	0	1	2	0	1
mod 4	1	2	3	0	1	2	3	0	1	2
mod 5	1	2	3	4	0	1	2	3	4	0
mod 6	1	2	3	4	5	0	1	2	3	4
mod 7	1	2	3	4	5	6	0	1	2	3
mod 8	1	2	3	4	5	6	7	0	1	2
mod 9	1	2	3	4	5	6	7	8	0	1
mod 10	1	2	3	4	5	6	7	8	9	0

是的，每个正整数具有 $1+1+\cdots+1$ 的形式．

29．

mod 3	2	1	0	2	1	0	2	1	0	2
mod 4	2	0	2	0	2	0	2	0	2	0
mod 5	2	4	1	3	0	2	4	1	3	0
mod 6	2	4	0	2	4	0	2	4	0	2
mod 7	2	4	6	1	3	5	0	2	4	6
mod 8	2	4	6	0	2	4	6	0	2	4
mod 9	2	4	6	8	1	3	5	7	0	2
mod 10	2	4	6	8	0	2	4	6	8	0

对于奇数模，数列 $2, 2+2, \cdots$ 包含所有剩余类．

对于模 $2k$，是 $2, 4, \cdots, 2(k-1), 0, 2, 4, \cdots$

对于模 $2k+1$，是 $2, 4, \cdots, 2k, 1, 3, \cdots, 2k-1, 0, \cdots$.

30.

mod 3	0	0	0	0	0	0	0	0	0	0
mod 4	3	2	1	0	3	2	1	0	3	2
mod 5	3	1	4	2	0	3	1	4	2	0
mod 6	3	0	3	0	3	0	3	0	3	0
mod 7	3	6	2	5	1	4	0	3	6	2
mod 8	3	6	1	4	7	2	5	0	3	6
mod 9	3	6	0	3	6	0	3	6	0	3
mod 10	3	6	9	2	5	8	1	4	7	0

对于不被 3 整除的模，数列 $3, 3+3, \cdots$ 包含所有剩余类.

对于模 $3k$，是 $3, 6, \cdots, 3(k-1), 0, 3, 6, \cdots$.

对于模 $3k+1$，是 $3, 6, \cdots, 3k, 2, 5, \cdots, 3k-1, 1, 4, \cdots, 3k-2, 0, \cdots$.

对于模 $3k+2$，是 $3, 6, \cdots, 3k, 1, 4, \cdots, 3k+1, 2, 5, \cdots, 3k-1, 0, 3, \cdots$.

31. 7, 11, 13.

32. $(\mathbf{Z}_2, +)$ 1,

$(\mathbf{Z}_4, +)$ 1, 3,

$(\mathbf{Z}_8, +)$ 1, 3, 5, 7,

$(\mathbf{Z}_{16}, +)$ 1, 3, 5, 7, 9, 11, 13, 15.

对模 2^k，任何偶数不能生成奇数.

$(\mathbf{Z}_{2^k}, +)$ 有 2^{k-1} 个生成元.

33. $(\mathbf{Z}_3, +)$ 1, 2,

$(\mathbf{Z}_9, +)$ 1, 2, 4, 5, 7, 8,

$(\mathbf{Z}_{27}, +)$ 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26.

对模 3^k，3 的任何倍数不能生成形如 $3n+1$ 的数.

$(\mathbf{Z}_{3^k}, +)$ 有 $2\cdot 3^{k-1}$ 个生成元.

34. $na+a\equiv a\ (\mathrm{mod}\ n)$, $na+ka\equiv ka\ (\mathrm{mod}\ n)$.

35. 数列中的第一个数.

36. 若$ka\equiv la\ (\mathrm{mod}\ n)$, 则$ka-la\equiv 0\ (\mathrm{mod}\ n)$, 从而$ka-la+a\equiv a\ (\mathrm{mod}\ n)$, $(k-l+1)a\equiv a\ (\mathrm{mod}\ n)$. 由于第$k$项是首次重复, 所以$k-l+1\geqslant k$, $l\leqslant 1$, 因此$l=1$.

37. 若$ka\equiv a\ (\mathrm{mod}\ n)$, 则$(k-1)a\equiv 0\ (\mathrm{mod}\ n)$, 于是$n|a(k-1)$. 设$\gcd(a,n)=1$, 则由问题1.61知道$n|k-1$. 但是$0<k-1<n$, 所以$n$不能是$k-1$的因数. 因此, a与n有公因数.

38. 若$\gcd(a,n)=d\neq 1$, 则对模n, a不能生成不被d整除的数.

由问题1.61知, 若$\gcd(a,n)=1$, 则$n|k-1$. 因此$k-1\geqslant n$, $k\geqslant n+1$. 可见数列的前n项是不同的. 所以a生成这个群.

上面的十九个问题都涉及定义群$(\mathbf{Z}_n, +)$并且确定它的生成元. 设数$a\in\mathbf{a}$, 以$\mathbf{0}, \mathbf{1}, \cdots, \mathbf{n-1}$表示模$n$的$n$个剩余类, 则当$\gcd(a,n)=1$时, $\mathbf{a}$必定是$(\mathbf{Z}_n, +)$的生成元.

39. $\varphi(1)=1$　1,

$\varphi(2)=1$　1,

$\varphi(3)=2$　1, 2,

$\varphi(4)=2$　1, 3,

$\varphi(5)=4$　1, 2, 3, 4,

$\varphi(6)=2$　1, 5,

$\varphi(7)=6$　1, 2, 3, 4, 5, 6,

$\varphi(8)=4$　1, 3, 5, 7,

$\varphi(9)=6$　1, 2, 4, 5, 7, 8,

$\varphi(10)=4$　1, 3, 7, 9.

40. $\varphi(2)=1$, $\varphi(4)=2$, $\varphi(8)=4$, $\varphi(16)=8$, $\varphi(32)=16$, $\varphi(64)=32$, $\varphi(128)=64$, $\varphi(256)=128$.

$\varphi(2^n) = 2^{n-1}$. 奇数是生成元，偶数不是.

41. $\varphi(3)=2$, $\varphi(9)=6$, $\varphi(27)=18$, $\varphi(81)=54$, $\varphi(243)=162$, $\varphi(3^n)=2\cdot 3^{n-1}$. 每第三个数有因数 3.

42. $\varphi(5)=4$, $\varphi(25)=20$, $\varphi(125)=100$, $\varphi(5^n)=4\cdot 5^{n-1}$. 每第五个数有因数 5.

43. $\varphi(p^n)=(p-1)p^{n-1}$. 当 p 为素数时，只有 p 的倍数才与p^n 有公因数，小于或等于 p^n 的这种数恰好有 p^{n-1} 个，所以

$\varphi(p^n)=p^n-p^{n-1}$.

记住这个结果很要紧.

44. $\varphi(2)\varphi(6)=2$, $\varphi(3)\varphi(4)=2\cdot 2=4=\varphi(12)$.

45. $\varphi(2)\varphi(9)=6=\varphi(18)$, $\varphi(3)\varphi(6)=4$.

46. $\varphi(2)\varphi(6)\neq\varphi(12)$.

若 $\gcd(a,b)=1$，则 $\varphi(ab)=\varphi(a)\varphi(b)$. 证明在下面的注记50.

47.

(0)	(9)	(6)	(3)
(4)	1	(10)	7
(8)	5	(2)	11

剩下了 $\varphi(3)$行，$\varphi(4)$列.

48.

(0)	(28)	(20)	(12)	(4)	(32)	(24)	(16)	(8)
(9)	1	29	(21)	13	5	(33)	25	17
(18)	(10)	(2)	(30)	(22)	(14)	(6)	(34)	(26)
(27)	19	11	(3)	31	23	(15)	7	35

剩下了 $\varphi(4)$行，$\varphi(9)$列.

49. 若两数有公因数，则必有一素公因数.有因数 2 的数恰好是与 0, 2, 4, 6, 8, 10, 12, 14 对模 16 同余的那些数. 有因数 3 的数恰好是与 0, 3, 6, 9, 12, 15, 18, 21, 24 对模 27 同余的那些数. 任何一个与 432 不互素的数有因数 2 或 3，或两者都有. 与 432 互素的数恰好是与 1, 3, 5, 7, 9, 11, 13, 15 对模 16 同余同时又与

1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26 对模 27 同余的那些数，因此，这种数有 $\varphi(16)\varphi(27)$个.

50. 如果 $\gcd(a, mn)=d\neq 1$，那么 d 必有某个素因数 p，于是 $p|mn$，所以 $p|m$ 或 $p|n$.

如果 $p|m$，那么与 a 在同一行的每个数都有因数 p，这是因为从 $a\equiv b \pmod m \Rightarrow b=a+mk$，所以 $p|b$.

类似地，如果 $p|n$，那么与 a 在同一列的每个数都有因数 p.

不全被删去的行数是 $\varphi(m)$.

不全被删去的列数是 $\varphi(n)$.

所以 $\varphi(mn)=\varphi(m)\varphi(n)$.

一当我们知道了对于任何素数 p 有 $\varphi(p^n)=p^n-p^{n-1}$，以及 φ 是积性函数，我们就可以利用算术基本定理对任意的 n 去确定 $\varphi(n)$的值. 这个技巧值得记住.

51. $\varphi(2^a3^b5^c)=\varphi(2^a3^b)\varphi(5^c)=\varphi(2^a)\varphi(3^b)\varphi(5^c)$.

52. 假设 $\varphi(p_1^{\alpha_1}\cdots p_{n-1}^{\alpha_{n-1}})=\varphi(p_1^{\alpha_1})\cdots\varphi(p_{n-1}^{\alpha_{n-1}})$成立，利用问题 50就可推出对有 n 个因数的情形也成立，所以由归纳法就证明了所要的结论.

54. 60/ 2 个数有因数 2.

60/ 3 个数有因数 3.

60/ 5 个数有因数 5.

60/ (2 · 3) 个数有因数 2 和 3.

60/ (2 · 5) 个数有因数 2 和 5.

60/ (3 · 5) 个数有因数 3 和 5.

60/ (2 · 3 · 5) 个数有因数 2 ,3 和 5.

$$\varphi(60)=60-\frac{60}{2}-\frac{60}{3}-\frac{60}{5}+\frac{60}{3\cdot 5}+\frac{60}{2\cdot 5}+\frac{60}{2\cdot 3}-\frac{60}{2\cdot 3\cdot 5}$$

$$=60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$=4\left(1-\frac{1}{2}\right)3\left(1-\frac{1}{3}\right)5\left(1-\frac{1}{5}\right)$$

$$=\varphi(4)\varphi(3)\varphi(5).$$

56. $$\varphi(p^a q^b r^c s^d)=p^a q^b r^c s^d\left(1-\frac{1}{p}-\frac{1}{q}-\frac{1}{r}-\frac{1}{s}+\frac{1}{pq}+\frac{1}{pr}+\frac{1}{ps}+\frac{1}{qr}+\frac{1}{qs}+\frac{1}{rs}-\frac{1}{qrs}-\frac{1}{rsp}-\frac{1}{spq}-\frac{1}{pqr}+\frac{1}{pqrs}\right)$$

$$=p^a q^b r^c s^d\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\left(1-\frac{1}{s}\right).$$

我们对 $\varphi(n)$ 的值的研究到此为止.

57. $\sum\limits_{d|6}\varphi(d)=6$, $\sum\limits_{d|8}\varphi(d)=8$, $\sum\limits_{d|12}\varphi(d)=12$.

58.

$\underline{1}$	2	3	4	$\underline{5}$	6	$\underline{7}$	8	9	10	$\underline{11}$	12
	$\underline{2}$	3	4		6		8	9	$\underline{10}$		12
		$\underline{3}$	4		6		8	$\underline{9}$			12
			$\underline{4}$		6		$\underline{8}$				12
					$\underline{6}$						12
											$\underline{12}$

若gcd $(a, 12)=d$ 而且 d 是12的第 i 个约数(按递增顺序),则 a 在第 i 行时被划线.

图2.1是对本题的图解,画出了经过原点而且斜率是 $\frac{n}{12}$ $(n=1, 2, \cdots, 12)$ 的那些直线. 每条直线上离原点最近的格点[①]被画上了圆圈.

① 平面上,两个坐标都是整数的点称为格点. —— 译者注.

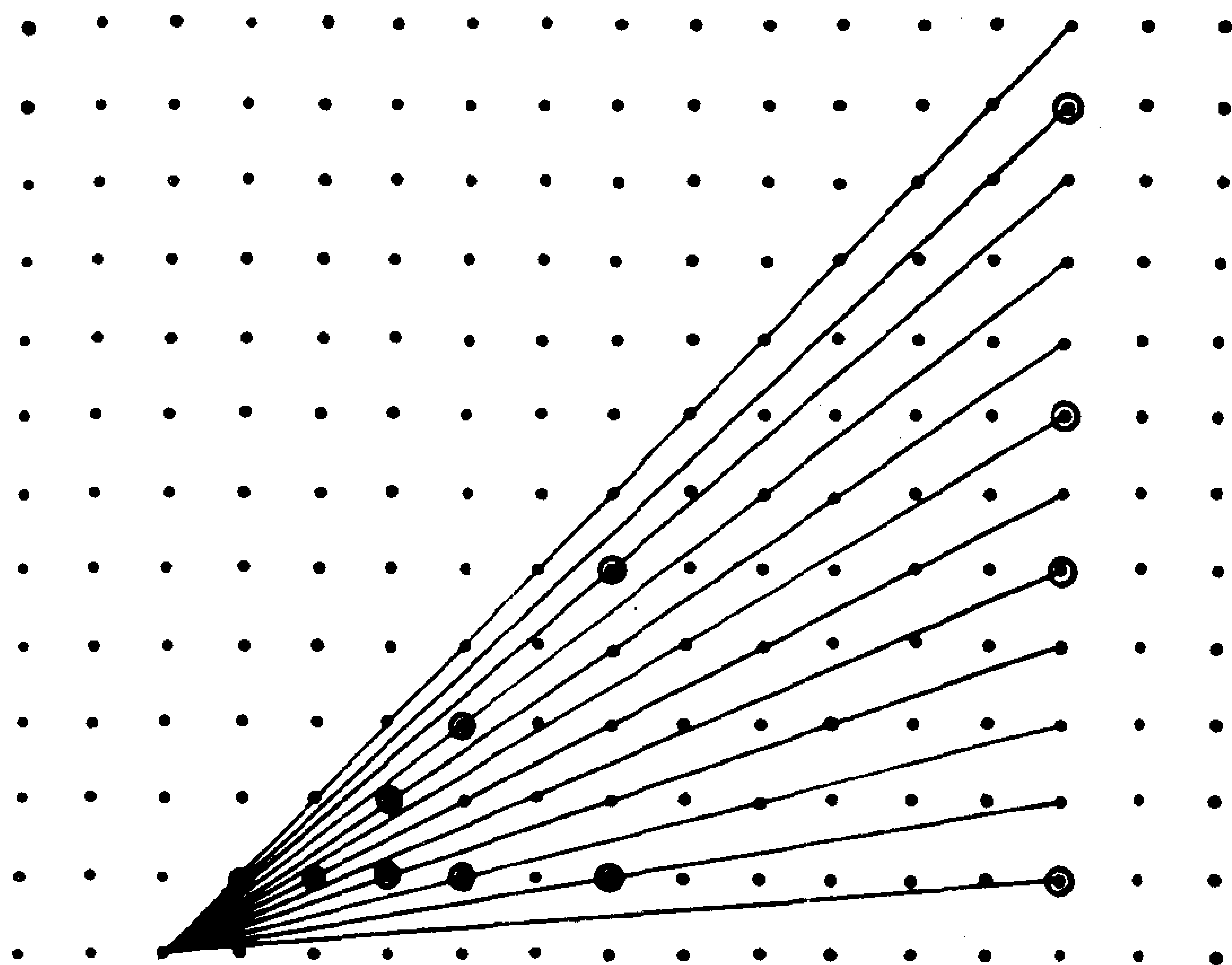


图 2.1

59. 若 $\gcd(a,n)=d_i$，则 a 在第 i 行时被划线. 数集 $\{x \mid 1 \leqslant x \leqslant n,\ \gcd(x,n)=d_i\}$ 与 $\varphi(\frac{n}{d_i})$ 个和 $\frac{n}{d_i}$ 互素的数一一对应.

60. $\sum_{d \mid 12} \varphi(d)=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)$

$\sum_{d \mid 12} \varphi(\frac{12}{d})=\varphi(12)+\varphi(6)+\varphi(4)+\varphi(3)+\varphi(2)+\varphi(1)$.

61. $f(p^\alpha)=\varphi(p^\alpha)+\varphi(p^{\alpha-1})+\cdots+\varphi(p)+\varphi(1)$

$=(p^\alpha-p^{\alpha-1})+(p^{\alpha-1}-p^{\alpha-2})+\cdots+(p-1)+1$

$=p^\alpha$.

建立等式 $f(p^\alpha)=p^\alpha$ 之后，只要能证明 f 是积性的，那就可以利用算术基本定理来确定 $f(n)$.

62. $f(9)f(8)=(\varphi(1)+\varphi(3)+\varphi(9))(\varphi(1)+\varphi(2)+\varphi(4)+\varphi(8))$

$$
\begin{aligned}
&= \varphi(1)\varphi(1)+\varphi(1)\varphi(2)+\varphi(1)\varphi(4)\\
&\quad+\varphi(1)\varphi(8)+\varphi(3)\varphi(1)+\varphi(3)\varphi(2)\\
&\quad+\varphi(3)\varphi(4)+\varphi(3)\varphi(8)+\varphi(9)\varphi(1)\\
&\quad+\varphi(9)\varphi(2)+\varphi(9)\varphi(4)+\varphi(9)\varphi(8)\\
&= \varphi(1)+\varphi(2)+\varphi(4)+\varphi(8)+\varphi(3)+\varphi(6)\\
&\quad+\varphi(12)+\varphi(24)+\varphi(9)+\varphi(18)+\varphi(36)+\varphi(72)\\
&=f(72).
\end{aligned}
$$

63. (i) 定义，(ii) 代数运算，(iii) φ 积性; m, n 互素，(iv) m, n 互素，(v) 定义.

这里的结果证明了f 是积性的.

64. $f(p_1^{\alpha_1}\cdots p_n^{\alpha_n})=f(p_1^{\alpha_1})\cdots f(p_n^{\alpha_n})$ (由问题 63)

$$=p_1^{\alpha_1}\cdots p_n^{\alpha_n}\ (\text{由问题61})$$

历 史 注 记

中国剩余定理是在中国和其他一些国家，大约在公元初年所提出的一类问题的通解. 虽然在1760 年，L .Euler发表他最早的一些算术论文时就用到了$\varphi(n)$，但现在所用的符号“$\varphi(n)$”是1801 年C .F.Gauss 在他的著作《Disquisitiones Arithmeticae》中引进的，而且，在这本书里发表了 $\sum\limits_{d|n}\varphi(d)=n$ 这个结果. 使用商群的语言与记号 $\mathbf{Z}_n$来研究算术性质，则是二十世纪的事了.

第三章 模 乘 法

Fermat 定 理

1．$6 \equiv 14 \pmod 4$ 且 $3 \equiv -1 \pmod 4$．$6 \cdot 3 \equiv 14(-1) \pmod 4$ 是否成立？

若 $a \equiv b \pmod 4$ 且 $c \equiv d \pmod 4$，能否证明 $ac \equiv bd \pmod 4$？

2．对模 4 的完全剩余系 $\{-4, 5, 2, -1\}$ 构造一个模 4 的乘法表．它与问题 1.14 中的表是否有相同结构？

3．设 $a \equiv b \pmod n$ 及 $c \equiv d \pmod n$，利用等式 $ac - bd = (a-b)c + b(c-d)$ 证明 $ac \equiv bd \pmod n$．

4．设 $a_1, \cdots, a_n$ 是模 n 的完全剩余系，当 $a_i a_j \equiv a_k \pmod n$ 时，定义 a_i 与 a_j 对模 n 的乘积为 a_k．a_k 是否唯一确定？

有没有元素 a_Z，使得对于所有的 i，$a_Z a_i \equiv a_Z \pmod n$？

有没有元素 a_I，使得对于所有的 i，$a_I a_i \equiv a_i \pmod n$？

5．设 $a_1, \cdots, a_n$ 与 $b_1, \cdots, b_n$ 都是 mod n 的完全剩余系，如何证明由这两个集合所得到的模 n 乘法表有相同结构？你的答案为 $(\mathbf{Z}_n, \times)$ 建立了一个合理的定义表．

6．检验表 3.1 中给出的对于模 3, 4, ⋯, 16 的乘法表，对于每个 n，$(\mathbf{Z}_n, \times)$ 中是否都有单位元？

7．比较关于 $(\mathbf{Z}_3, \times)$，$(\mathbf{Z}_4, \times)$，⋯，$(\mathbf{Z}_{10}, \times)$ 的这些表中的第二行与问题 2.28 的答案，它们有什么相似之处？

8．比较关于 $(\mathbf{Z}_3, \times)$，$(\mathbf{Z}_4, \times)$，⋯，$(\mathbf{Z}_{10}, \times)$ 的这些表的第三行与问题 2.29 的答案，有何相似之处？

表 3.1

模 3 乘法

0	0	0
0	1	2
0	2	1

模 4 乘法

0	0	0	0
0	1	2	3
0	2	0	2
0	3	2	1

模 5 乘法

0	0	0	0	0
0	1	2	3	4
0	2	4	1	3
0	3	1	4	2
0	4	3	2	1

模 6 乘法

0	0	0	0	0	0
0	1	2	3	4	5
0	2	4	0	2	4
0	3	0	3	0	3
0	4	2	0	4	2
0	5	4	3	2	1

模 7 乘法

0	0	0	0	0	0	0
0	1	2	3	4	5	6
0	2	4	6	1	3	5
0	3	6	2	5	1	4
0	4	1	5	2	6	3
0	5	3	1	6	4	2
0	6	5	4	3	2	1

模 8 乘法

0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7
0	2	4	6	0	2	4	6
0	3	6	1	4	7	2	5
0	4	0	4	0	4	0	4
0	5	2	7	4	1	6	3
0	6	4	2	0	6	4	2
0	7	6	5	4	3	2	1

模 9 乘法

0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8
0	2	4	6	8	1	3	5	7
0	3	6	0	3	6	0	3	6
0	4	8	3	7	2	6	1	5
0	5	1	6	2	7	3	8	4
0	6	3	0	6	3	0	6	3
0	7	5	3	1	8	6	4	2
0	8	7	6	5	4	3	2	1

模 10 乘法

0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9
0	2	4	6	8	0	2	4	6	8
0	3	6	9	2	5	8	1	4	7
0	4	8	2	6	0	4	8	2	6
0	5	0	5	0	5	0	5	0	5
0	6	2	8	4	0	6	2	8	4
0	7	4	1	8	5	2	9	6	3
0	8	6	4	2	0	8	6	4	2
0	9	8	7	6	5	4	3	2	1

模 11 乘法

0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10
0	2	4	6	8	10	1	3	5	7	9
0	3	6	9	1	4	7	10	2	5	8
0	4	8	1	5	9	2	6	10	3	7
0	5	10	4	9	3	8	2	7	1	6
0	6	1	7	2	8	3	9	4	10	5
0	7	3	10	6	2	9	5	1	8	4
0	8	5	2	10	7	4	1	9	6	3
0	9	7	5	3	1	10	8	6	4	2
0	10	9	8	7	6	5	4	3	2	1

模 12 乘法

0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11
0	2	4	6	8	10	0	2	4	6	8	10
0	3	6	9	0	3	6	9	0	3	6	9
0	4	8	0	4	8	0	4	8	0	4	8
0	5	10	3	8	1	6	11	4	9	2	7
0	6	0	6	0	6	0	6	0	6	0	6
0	7	2	9	4	11	6	1	8	3	10	5
0	8	4	0	8	4	0	8	4	0	8	4
0	9	6	3	0	9	6	3	0	9	6	3
0	10	8	6	4	2	0	10	8	6	4	2
0	11	10	9	8	7	6	5	4	3	2	1

模 13 乘法

0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12
0	2	4	6	8	10	12	1	3	5	7	9	11
0	3	6	9	12	2	5	8	11	1	4	7	10
0	4	8	12	3	7	11	2	6	10	1	5	9
0	5	10	2	7	12	4	9	1	6	11	3	8
0	6	12	5	11	4	10	3	9	2	8	1	7
0	7	1	8	2	9	3	10	4	11	5	12	6
0	8	3	11	6	1	9	4	12	7	2	10	5
0	9	5	1	10	6	2	11	7	3	12	8	4
0	10	7	4	1	11	8	5	2	12	9	6	3
0	11	9	7	5	3	1	12	10	8	6	4	2
0	12	11	10	9	8	7	6	5	4	3	2	1

模 14 乘法

0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	2	4	6	8	10	12	0	2	4	6	8	10	12
0	3	6	9	12	1	4	7	10	13	2	5	8	11
0	4	8	12	2	6	10	0	4	8	12	2	6	10
0	5	10	1	6	11	2	7	12	3	8	13	4	9
0	6	12	4	10	2	8	0	6	12	4	10	2	8
0	7	0	7	0	7	0	7	0	7	0	7	0	7
0	8	2	10	4	12	6	0	8	2	10	4	12	6
0	9	4	13	8	3	12	7	2	11	6	1	10	5
0	10	6	2	12	8	4	0	10	6	2	12	8	4
0	11	8	5	2	13	10	7	4	1	12	9	6	3
0	12	10	8	6	4	2	0	12	10	8	6	4	2
0	13	12	11	10	9	8	7	6	5	4	3	2	1

模 15 乘法

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
0	9	3	12	6	0	9	3	12	6	0	9	3	12	6
0	10	5	0	10	5	0	10	5	0	10	5	0	10	5
0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

模 16 乘法

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	4	6	8	10	12	14	0	2	4	6	8	10	12	14
0	3	6	9	12	15	2	5	8	11	14	1	4	7	10	13
0	4	8	12	0	4	8	12	0	4	8	12	0	4	8	12
0	5	10	15	4	9	14	3	8	13	2	7	12	1	6	11
0	6	12	2	8	14	4	10	0	6	12	2	8	14	4	10
0	7	14	5	12	3	10	1	8	15	6	13	4	11	2	9
0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8
0	9	2	11	4	13	6	15	8	1	10	3	12	5	14	7
0	10	4	14	8	2	12	6	0	10	4	14	8	2	12	6
0	11	6	1	12	7	2	13	8	3	14	9	4	15	10	5
0	12	8	4	0	12	8	4	0	12	8	4	0	12	8	4
0	13	10	7	4	1	14	11	8	5	2	15	12	9	6	3
0	14	12	10	8	6	4	2	0	14	12	10	8	6	4	2
0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

9. 比较关于 $(\mathbf{Z}_3,\times)$, $(\mathbf{Z}_4,\times)$, …, $(\mathbf{Z}_{10},\times)$ 的这些表的第四行与问题 2.30 的答案, 有何相似之处?

10. 关于 $(\mathbf{Z}_n,\times)$ 的表的第 $a+1$ 行与数列 $a, a+a, \cdots \pmod n$ 的项之间有何相似之处?

11. 数列 $a, a+a, a+a+a, \cdots \pmod n$ 中, 哪一项在第一次重复的项之前?

12. 在表 3.1 中, 对于哪些模 $n=3, 4, \cdots, 16$, $(\mathbf{Z}_n,\times)$ 中有不在第一行或第一列的零元素?

13. 设 n 是合数, 说明必有 $(\mathbf{Z}_n,\times)$ 的零元素不在第一行或第一列的原因; 证明含有两个零元素的行或列不会含有 $\mathbf{Z}_n$ 的全部元素.

14. 设 p 是素数, 利用问题 2.38 来说明 $(\mathbf{Z}_p,\times)$ 的表的每一行[①]都含有 $\mathbf{Z}_p$ 的全部元素. 这就是说, 若 $0<a<p$, 则对应 $x\to ax$ 是 $\mathbf{Z}_p$ 中元素的一个置换.

证明: 从 $ax=ay \pmod p$ 可推导出 $x\equiv y \pmod p$; 再若 $0<b<p$, 则在 0 与 p 之间存在唯一的 x, 使得 $ax\equiv b \pmod p$.

15. 设 p 是素数, $0<a<p$. 集合 $\{1, 2, \cdots, p-1\}$ 与 $\{a, 2a, \cdots, (p-1)a\}$ 是否都含有 $\mathbf{Z}_p$ 的全部非零元素?

将每个集合的全部元素相乘并比较这两个乘积, 你能得到什么结论? 利用问题 14 中建立的相约性证明 $a^{p-1}\equiv 1 \pmod p$.

16. 利用问题 14 证明, $(\mathbf{Z}_p,\times)$ 中的每一个非零元素都有乘法逆元素. 就是说, 对于每个 $x\not\equiv 0 \pmod p$, 存在 $a\not\equiv 0 \pmod p$, 使得 $ax\equiv 1 \pmod p$.

17. $\mathbf{Z}_p$ 的非零元素在模 p 的乘法下是否构成群?

18. 利用 Lagrange 定理 (子群的阶整除群的阶) 证明, 对于 $\mathbf{Z}_p$ 的任何非零元素 x 有 $x^{p-1}=1$.

---

① 第一行除外. —— 译者注.

19. 利用问题 15 或问题18 证明：对于所有整数x与所有素数p有$x^p \equiv x \pmod{p}$ (Fermat 定理).

20. 证明$2222^{5555}+5555^{2222}$被 7 整除 . 你自己提出一个类似的问题.

Wilson 定 理

21. 对于素数p，以M_p表示Z_p的非零元素所成的集合，这样，$(M_p, \times)$就构成一个群. 在群M_3, M_5, M_7, M_{11}及M_{13}中，求使$x^2=1$的元素x. 推广你的结论，并找出M_p中使得$x^2=1$的元素x.

22. 在M_7中，$2 \cdot 4=1$而且$3 \cdot 5=1$.由此证明

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 6 \pmod{7}.$$

23. 计算$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \pmod{11}$.

24. 在M_p中，元素$1, 2, \cdots, p-1$中有多少个与自己的乘法逆元素不相等？

25. 计算乘积$(p-1)! \pmod{p}$ (Wilson 定理).

一次同余方程

26. 利用表 3.1 求下列方程的解 (如果存在的话):

$$4x \equiv 10 \pmod{14},$$

$$4x \equiv 9 \pmod{14},$$

$$9x \equiv 2 \pmod{14}.$$

27. b取何值时，方程

$$4x \equiv b \pmod{14}$$

(i) 在 $0 \leqslant x < 14$ 中有多于一个的解? (ii) 无解?

28. 设 b 是奇数，用式子证明不存在整数 x，使得 $4x \equiv b \pmod{14}$.

29. 设 b 是偶数 ($b = 2c$)，同余方程 $4x \equiv 2c \pmod{14}$ 与 $2x \equiv c \pmod{7}$ 是否等价? 证明: 从 $2x = c \pmod{7}$ 对模 7 的唯一解能导出 $4x \equiv b \pmod{14}$ 的两个解.

30. 设 $ax \equiv b \pmod{n}$ 对 x 有解，证明 $\gcd(a, n) | b$.

31. 若 $\gcd(a, n) = 1$，则由问题 1.34 知，存在整数 r，s，使得 $ar + ns = 1$. 证明对于任何数 b，br 是方程 $ax \equiv b \pmod{n}$ 的解.

32. 设 $\gcd(a, n) = 1$，$ax \equiv b \pmod{n}$ 以及 $ay \equiv b \pmod{n}$，证明 $x \equiv y \pmod{n}$.

33. 利用问题31和问题32 证明，若 $\gcd(a, n) = d | b$，则 $\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ 有唯一解 $\pmod{\frac{n}{d}}$. 证明 $ax \equiv b \pmod{n}$ 有 d 个对模 n 不同余的解.

Fermat－Euler 定理

现在，我们要将 Fermat 定理推广到任意模的情形，即模不一定是素数. 这一推广基于在 $(Z_n, \times)$ 内找一个群.

34. 利用表 3.1 列出使

$$ax \equiv 1 \pmod{14}$$

有解的所有的值 a.

利用表 3.1 列出使对应 $x \to ax$ 是 Z_{14} 中元素的置换的所有的值 a.

如何解释这两个集合的相似性?

35. 利用表 3.1 列出使

$$ax \equiv 1 \pmod{12}$$

有解的所有的值 a；列出使对应

$$x \to ax$$

是 Z_{12} 中元素的置换的所有的值 a.

36. 设 $n \geqslant 2$. 证明集合 $\{1, 2, \cdots, n-1\}$ 的下述三个子集的等价性:

(i) $\{a \mid \gcd(a, n) = 1\}$,

(ii) $\{a \mid ax \equiv 1 \pmod{n}$ 有解$\}$,

(iii) $\{a \mid x \to ax$ 是 Z_n 的一个置换$\}$.

每个子集中有多少元素? 这种集合称为模 n 的简化剩余系，用 M_n 表示.

37. 证明当 n 是素数时，上题中 M_n 的定义和问题21中 M_p 的定义是一致的.

38. 对 $n = 4, 6, 8, 9, 10$，写出 M_n 的乘法表.

39. 上题中所得到的表是否都是群的定义表？

40. 利用问题 36 中 M_n 的第二个定义，证明 $(M_n, \times)$ 是群.

41. 设 $a_1, a_2, \cdots, a_{\varphi(n)}$ 是模 n 的简化剩余系，利用上题证明 $a_i a_1, a_i a_2, \cdots, a_i a_{\varphi(n)}$ 也是模 n 的简化剩余系. 通过考察每个集合的元素的乘积，证明 $a_i^{\varphi(n)} \equiv 1 \pmod{n}$ (Fermat – Euler 定理).

42. 利用关于子群的 Lagrange 定理，证明当 $\gcd(a, n) = 1$ 时，$a^{\varphi(n)} \equiv 1 \pmod{n}$.

联立一次同余方程

43. 如果可能，求出下面联立方程的解 (mod 30):

(i) $x \equiv 1 \pmod{3}$, $2x \equiv 4 \pmod{10}$;

(ii) $x \equiv 1 \pmod{3}$, $2x \equiv 3 \pmod{10}$;

(iii) $x \equiv 1 \pmod{3}$,
$3x \equiv 1 \pmod{10}$;

(iv) $x \equiv 1 \pmod{3}$,
$3x \equiv 2 \pmod{10}$.

44. 叙述使方程组

$$a_1x \equiv b_1 \pmod{m_1},$$
$$a_2x \equiv b_2 \pmod{m_2}$$

有唯一解 $\pmod{m_1m_2}$的条件.

关于多项式的Lagrange定理

45. 用表3.2判断方程 $x^2 \equiv 1 \pmod{n}$是否有两个以上的解 $\pmod{n}$，其中 $n = 3, 4, 5, \cdots, 16$. 为什么问题21中所用的论证不能用于此处的每一种情形?

46. 对于模 $n = 5, 7, 11$ 及 13，利用表3.2 判断 $x^3 \equiv 1 \pmod{n}$有多少解?

计算乘积 $(x-1)(x-2)(x-4) \pmod{7}$与

$$(x-1)(x-3)(x-9) \pmod{13}.$$

证明方程 $x^2 + x + 1 \equiv 0$ 对于 mod 5 与 mod 11 均无解.

47. 对于模 $n = 5, 7, 11$ 及 13，利用表3.2 判断 $x^4 \equiv 1 \pmod{n}$有多少解?

计算乘积 $(x-1)(x-2)(x-3)(x-4) \pmod{5}$与

$$(x-1)(x-5)(x-8)(x-12) \pmod{13}.$$

将 $x^4 - 1$ 分解因式，并证明 $x^2 + 1 \equiv 0$ 对 mod 7 与mod 11都无解.

表 3.2

对模 3 的幂

0	0
1	1
2	1

对模 4 的幂

0	0	0
1	1	1
2	0	0
3	1	3

对模 5 的幂

0	0	0	0
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1

对模 6 的幂

0	0	0	0	0
1	1	1	1	1
2	4	2	4	2
3	3	3	3	3
4	4	4	4	4
5	1	5	1	5

对模 7 的幂

0	0	0	0	0	0
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

对模 8 的幂

0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	0	0	0	0	0
3	1	3	1	3	1	3
4	0	0	0	0	0	0
5	1	5	1	5	1	5
6	4	0	0	0	0	0
7	1	7	1	7	1	7

对模9的幂

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	8	7	5	1	2	4
3	0	0	0	0	0	0	0
4	7	1	4	7	1	4	7
5	7	8	4	2	1	5	7
6	0	0	0	0	0	0	0
7	4	1	7	4	1	7	4
8	1	8	1	8	1	8	1

对模 10 的幂

0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
2	4	8	6	2	4	8	6	2
3	9	7	1	3	9	7	1	3
4	6	4	6	4	6	4	6	4
5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6
7	9	3	1	7	9	3	1	7
8	4	2	6	8	4	2	6	8
9	1	9	1	9	1	9	1	9

对模 11 的幂

0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

对模 12 的幂

0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
2	4	8	4	8	4	8	4	8	4	8
3	9	3	9	3	9	3	9	3	9	3
4	4	4	4	4	4	4	4	4	4	4
5	1	5	1	5	1	5	1	5	1	5
6	0	0	0	0	0	0	0	0	0	0
7	1	7	1	7	1	7	1	7	1	7
8	4	8	4	8	4	8	4	8	4	8
9	9	9	9	9	9	9	9	9	9	9
10	4	4	4	4	4	4	4	4	4	4
11	1	11	1	11	1	1	1	11	1	11

对模 13 的幂

0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	1
3	9	1	3	9	1	3	9	1	3	9	1
4	3	12	9	10	1	4	3	12	9	10	1
5	12	8	1	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	1
7	10	5	9	11	12	6	3	8	4	2	1
8	12	5	1	8	12	5	1	8	12	5	1
9	3	1	9	3	1	9	3	1	9	3	1
10	9	12	3	4	1	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1

对模 14 的幂

0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	2	4	8	2	4	8	2	4	8	2
3	9	13	11	5	1	3	9	13	11	5	1	3
4	2	8	4	2	8	4	2	8	4	2	8	4
5	11	13	9	3	1	5	11	13	9	3	1	5
6	8	6	8	6	8	6	8	6	8	6	8	6
7	7	7	7	7	7	7	7	7	7	7	7	7
8	8	8	8	8	8	8	8	8	8	8	8	8
9	11	1	9	11	1	9	11	1	9	11	1	9
10	2	6	4	12	8	10	2	6	4	12	8	10
11	9	1	11	9	1	11	9	1	11	9	1	11
12	4	6	2	10	8	12	4	6	2	10	8	12
13	1	13	1	13	1	13	1	13	1	13	1	13

对模 15 的幂

0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	1	2	4	8	1	2	4	8	1	2	4
3	9	12	6	3	9	12	6	3	9	12	6	3	9
4	1	4	1	4	1	4	1	4	1	4	1	4	1
5	10	5	10	5	10	5	10	5	10	5	10	5	10
6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	4	13	1	7	4	13	1	7	4	13	1	7	4
8	4	2	1	8	4	2	1	8	4	2	1	8	4
9	6	9	6	9	6	9	6	9	6	9	6	9	6
10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	1	11	1	11	1	11	1	11	1	11	1	11	1
12	9	3	6	12	9	3	6	12	9	3	6	12	9
13	4	7	1	13	4	7	1	13	4	7	1	13	4
14	1	14	1	14	1	14	1	14	1	14	1	14	1

对模 16 的幂

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	0	0	0	0	0	0	0	0	0	0	0	0
3	9	11	1	3	9	11	1	3	9	11	1	3	9	11
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	9	13	1	5	9	13	1	5	9	13	1	5	9	13
6	4	8	0	0	0	0	0	0	0	0	0	0	0	0
7	1	7	1	7	1	7	1	7	1	7	1	7	1	7
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	1	9	1	9	1	9	1	9	1	9	1	9	1	9
10	4	8	0	0	0	0	0	0	0	0	0	0	0	0
11	9	3	1	11	9	3	1	11	9	3	1	11	9	3
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	9	5	1	13	9	5	1	13	9	5	1	13	9	5
14	4	8	0	0	0	0	0	0	0	0	0	0	0	0
15	1	15	1	15	1	15	1	15	1	15	1	15	1	15

48．对于模 $n=7, 11$ 及 13，利用表 3.2 判断 $x^5 \equiv 1 \pmod{n}$ 有多少解？

计算乘积 $(x-1)(x-3)(x-4)(x-5)(x-9) \pmod{11}$.

证明 $x^4+x^3+x^2+x+1 \equiv 0$ 对 mod 7 与 mod 13 都是无解.

49．求多项式 $g(x)$，使得 $x^n-1=(x-1)g(x)$，其中 $n \geqslant 2$ 是正整数.

50．求多项式 $g(x)$，使得 $x^n-a^n=(x-a)g(x)$，其中 $n \geqslant 2$ 是正整数.

51．设 $f(x)$ 是 n 次多项式，证明 $f(x)-f(a)$ 可以表示为 $x-a$ 与一个 $n-1$ 次多项式之积. 证明：若 $f(a) \equiv 0$，则 $f(x)$ 有因式 $x-a$. 同样证明：若 $f(x)$ 是整系数多项式且 $f(a) \equiv 0 \pmod{p}$，则 $f(x) \equiv (x-a)g(x) \pmod{p}$，其中 $g(x)$ 是 $n-1$ 次整系数多项式.

52．能否选取整数 k, l, m, n, p, q，使得多项式

$$
\begin{aligned}
&(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)\\
&+k(x-1)(x-2)(x-3)(x-4)(x-5)\\
&+l(x-1)(x-2)(x-3)(x-4)\\
&+m(x-1)(x-2)(x-3)\\
&+n(x-1)(x-2)\\
&+p(x-1)\\
&+q
\end{aligned}
$$

等于 x^6-1? (不必计算实际数值). 利用 Fermat 定理证明 $x=1, 2, 3, 4, 5, 6$ 都满足 $x^6-1\equiv 0 \pmod 7$, 从而导出

$$0\equiv q\equiv p\equiv n\equiv m\equiv l\equiv k \pmod 7.$$

证明 $x^6-1\equiv(x-1)(x-2)(x-3)(x-4)(x-5)(x-6) \pmod 7$.

53. 能否用类似于上题的方法, 将 $x^{10}-1 \pmod{11}$ 因式分解?

能否用类似于上题的方法, 将 $x^{12}-1 \pmod{13}$ 因式分解?

用类似于上题的方法, 将 $x^{p-1}-1 \pmod p$ 因式分解, 其中 p 是任一素数.

当 p 是奇素数时, 通过考察上面最后一个因式分解中的常数项, 给出 Wilson 定理 (问题 25) 的另一证明.

54. 如果 x^3-1 有三个不同的零点 $a, b, c \pmod{19}$[①], 用类似于问题 52 中的方法证明

$$x^3-1\equiv (x-a)(x-b)(x-c) \pmod{19}.$$

x^3-1 能否有不与 a, b, c 同余的第四个零点 $d \pmod{19}$?

55. 设 p 是素数, 证明 x^3-1 不能有四个不同的零点 $\pmod p$.

56. 设 n 是正整数, 素数 p 大于 n. x^n-1 至多有几个不同的零点 $\pmod p$?

---

① 即 $x^3-1\equiv 0 \pmod{19}$ 有三个对模19 互不同余的解 a, b, c. —— 译者注.

57. 用上题方法证明：整系数多项式 $a_0x^n+a_1x^{n-1}+\cdots+a_n$ $(a_0\neq 0)$至多有 n 个不同的零点 (关于多项式的 Lagrange 定理).

我们将要利用这个很重要的定理来证明素数模的原根的存在性 (问题 59, 60, 61)以及 Chevalley 定理 (问题 75 − 87).

原　根

58. 对于 $p=3,5,7,11,13$ 利用表3.2 求 $(M_p,\times)$中每个元素的阶. 证明这些阶分别是 2, 4, 6, 10, 12 的因数. 这些乘法群 $(M_p,\times)$是否都是循环群?

59. 若群$(M_p,\times)$含有一个阶为 d 的元素 a , d 与 $p-1$ 有何关系?

利用元素 a 构造 $x^d-1\equiv 0 \pmod p$的 d 个不同的解. 为什么这个方程不存在另外的解? $x^d-1\equiv 0 \pmod p$ 的这 d 个解是否构成 $(M_p,\times)$的一个循环子群? 利用“含有 d 个元素的循环群与加法群 $(Z_d,+)$有相同结构”这个事实，证明这样的循环群含有 $\varphi(d)$个生成元；进而证明，只要$(M_p,\times)$含有某个 d 阶元素，它就恰好含有 $\varphi(d)$ 个 d 阶元素.

60. 以 N_d 表示群$(M_p,\times)$中 d 阶元素的个数,利用上题说出 N_d 的取值情况.

若 d 不是$p-1$ 的因数，证明 $N_d=0$.

61. 设 $d_1,\cdots,d_k$ 是 $p-1$ 的全部约数 (包括 1 和 $p-1$)，将$(M_p,\times)$ 的元素按它们的阶分类，证明

$$N_{d_1}+N_{d_2}+\cdots+N_{d_k}=p-1\ .$$

利用问题 2.64 证明

$$\varphi(d_1)+\varphi(d_2)+\cdots+\varphi(d_k)=p-1\ .$$

利用问题 60 证明: $N_d=\varphi(d)$对于$p-1$ 的任一约数 d 成立，从而$N_{p-1}=\varphi(p-1)$.

因为在 $(M_p,\times)$ 中有 $p-1$ 阶元素，所以 $(M_p,\times)$ 是循环群.

这是关于原根的关键性结果. 问题62－74要更细致地考察群 $(M_n,\times)$，指出这些群中哪一些是循环群. 但这些结果在以后的几章中并不需要. 只有当 $(M_n,\times)$ 是循环群时，模 n 的原根才存在.

62. 用表3.2来检验群 $(M_n,\times)$ $(n=4,6,8,9,10,12,14,15,16)$，指出哪些是循环群，哪些不是？ $(M_n,\times)$ 的生成元称为模 n 的原根.

63. 看问题2.47并回忆删去不与12互素的那些数的过程.

(0)	(9)	(6)	(3)
(4)	1	(10)	7
(8)	5	(2)	11

在含有1的那一列，剩下的未划线的数是否构成模3的简化剩余系？

在含有1的那一行，剩下的未划线的数是否构成模4的简化剩余系？

未划线的数的排列是否像是模12乘法表的一部分？

$1\cdot 1$	$1\cdot 7$
$5\cdot 1$	$5\cdot 7$

乘法群 M_{12} 可否表示为群 M_3 与 M_4 的直积？

64. 利用问题2.48中的表，并选择群 $(M_4,\times)$ 与 $(M_9,\times)$ 的适当形式[①]使得群 M_{36} 中的每个元素都可表为这两个群的元素之积. 对模9和模4，考虑乘积 $19\cdot 25$，不计算它的数值，证明 $19\cdot 25\equiv 7 \pmod{36}$.

65. 推广问题63与64中的方法，证明若 $\gcd(m,n)=1$，则 $M_{mn}=M_m\times M_n$.

---

① 例如：1，3；1，7都可看作是群 $(M_4,\times)$ 的具体形式. —— 译者注.

特别注意证明：若 $a \equiv 1 \pmod{m}$ 及 $b \equiv 1 \pmod{n}$，则 $ab \equiv b \pmod{m}$ 及 $ab \equiv a \pmod{n}$.

66. 从 M_{63} 中选两个集合，使得其中一个是模 7 的简化剩余系，另一个是模 9 的简化剩余系，并且可将 M_{63} 表示为 M_7 和 M_9 的直积. 找一个 M_{63} 的子群，使其含有 9 个阶为 1 或 3 的元素.

67. 若 n 是奇数，为什么 $(M_{2n}, \times)$ 与 $(M_n, \times)$ 有相同的构造？

68. 数 2 是模 3, 9, 27 及 81 的原根，利用这点，求这些模的所有原根，即求出群 M_3, M_9, M_{27} 及 M_{81} 的所有生成元；用描图纸或复制下表，把在下面表中的这些数圈出来：

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81

显然，模 9, 27, 81 的每个原根都与 $2 \pmod{3}$ 同余.

69. 证明对于所有整数 k，

$$(3k+1)^3 \equiv 1 \pmod{9},$$

$$(3k+1)^9 \equiv 1 \pmod{27},$$

$$(3k+1)^{27} \equiv 1 \pmod{81},$$

进而对 n 实行归纳法，推出 $(3k+1)^{3^n} \equiv 1 \pmod{3^{n+1}}$.

证明对于任何 n，与 1 同余 $\pmod{3}$ 的数不会是模 3^n 的原根.

70. 设 p 是奇素数，$a \in M_p$ 但不是模 p 的原根，即 $a^d \equiv 1 \pmod{p}$，$0<d<p-1$，证明：

(i) $(pk+a)^d \equiv 1 \pmod{p}$,

(ii) $(pk+a)^d \equiv 1+hp \pmod{p^2}$,

(iii) $(pk+a)^{dp} \equiv 1 \pmod{p^2}$,

(iv) $(pk+a)^{dp^2} \equiv 1 \pmod{p^3}$,

其中k是任意整数，h是整数. 证明与a同余$(\bmod\ p)$的数不能是模p^2或p^3的原根.

71. 在求模3^n的形如$3k+2$的原根时，为什么由条件

$$(3k+2)^2 \equiv 1 \pmod{9} \text{ 或 } (3k+2)^3 \equiv 1 \pmod{9}$$

就能断定$3k+2$不是模9的原根? 用 Fermat 定理证明$(3k+2)^3 \not\equiv 1 \pmod{9}$. 证明$(3k+2)^2 \not\equiv 1 \pmod{9}$是使$3k+2$成为模9的原根的充分条件. k的哪些值满足这个条件?

72. 设a是模p的原根，p是奇素数，为什么由条件

$$(pk+a)^{pd} \equiv 1 \pmod{p^2},\quad 0<d<p-1$$

或 $$(pk+a)^{p-1} \equiv 1 \pmod{p^2}$$

就能断定$pk+a$不是 mod p^2的原根? 反之，当这两个条件都不成立时，$pk+a$就是 mod p^2的原根，为什么?

证明 $(pk+a)^{pd} \not\equiv 1 \pmod{p^2}$.

利用 $(a+pk)^{p-1}=a^{p-1}+(p-1)a^{p-2}pk+p^2(\cdots)$

$$\equiv a^{p-1}-a^{p-2}pk \pmod{p^2}$$

$$\equiv 1+ph-a^{p-2}pk \pmod{p^2}$$

(h是某个整数)，指出如何选取k，使得$a+pk$是模p^2的原根.

73. 设$(pk+a)^{p-1}=1+pu$，其中u不被p整除(所以$pk+a$是模p^2的原根)，证明$(pk+a)^{p(p-1)}=1+p^2v$，其中v不被p整除，从而推出$pk+a$也是模p^3的原根.

74. 设p是奇素数，a是模p^n的原根，证明数a与$a+p^n$中的奇数是模$2p^n$的原根.

在本章最后的十二个问题中，我们将把关于多项式的 Lagrange 定理推广到多个变量的情形，并且证明某些多项式方

程的非零解的存在性.

Chevalley 定 理

75. 对于模 $n=3,5$ 及 7，求 $x^2+y^2+z^2\equiv 0 \pmod{n}$ 的异于 $(x,y,z)\equiv(0,0,0) \pmod{n}$[1] 的解.

76. 假设对于某个素数 p，除 $(x,y,z)\equiv(0,0,0)$ 外 $x^2+y^2+z^2\equiv 0 \pmod{p}$ 无解. 利用 Fermat 定理证明，对于所有整数 x,y,z 有

$$(x^2+y^2+z^2)^{p-1}\equiv 1-(1-x^{p-1})(1-y^{p-1})(1-z^{p-1}) \pmod{p}$$

77. 规定多项式的项 $x^ay^bz^c$ 的次数是 $a+b+c$. $(x^2+y^2+z^2)^{p-1}$ 的项的最高次数是多少? 写出 $1-(1-x^{p-1})(1-y^{p-1})(1-z^{p-1})$ 的最高次项.

78. 说明为什么任一 x 的多项式对模 p 等价于一个次数 $\leqslant p-1$ 的多项式，就是说，对于每一个整系数多项式 $f(x)$，存在一个次数 $\leqslant p-1$ 的整系数多项式 $g(x)$，使得 $f(x)\equiv g(x) \pmod{p}$ 对一切整数 x 成立.

79. 设 $f(x)$ 与 $g(x)$ 是两个次数 $\leqslant p-1$ 的整系数多项式，证明: $f(x)\equiv g(x) \pmod{p}$ 对一切整数 x 成立的充要条件是 $f(x)$ 与 $g(x)$ 中次数相同的项的系数对模 p 同余.

80. 利用上题证明: 若 $f(x,y)$ 与 $g(x,y)$ 是整系数多项式，它们所含的 x 或 y 的幂次都不超过 $p-1$，而且 $f(x,y)\equiv g(x,y) \pmod{p}$ 对于一切整数 x,y 成立，则 f 与 g 中 x^iy^j 项的系数对模 p 同余.

81. 怎样推广上题的论证，对三个变量 x,y,z 的多项式来证明一个类似的结论?

---

[1] $(x,y,z)\equiv(0,0,0) \pmod{p}$ 表示 $x\equiv 0 \pmod{n}$ $y\equiv 0 \pmod{n}$ $z\equiv 0 \pmod{n}$ 同时成立. 在不会混淆时，"$(\mathrm{mod}\ n)$" 可不写出来.——译者注.

82. 将上题结果用于问题77，证明问题 76 中的假设条件是错误的.

83. 在方程 $xyz+x^2+y^2+z^2\equiv 0 \pmod p$ 只有解 $(x,y,z)\equiv(0,0,0)$ 的假设下，像问题76那样，求一个与 $(xyz+x^2+y^2+z^2)^{p-1}$ 对模 p 等价的多项式. 在这种情况下，为什么没有类似于问题 77 的结果? (注意: 对模3只有零解).

84. 在 $(1,1,1) \pmod p$ 是方程 $x^2+y^2+z^2-3\equiv 0 \pmod p$ 的唯一解的假设下，试将问题 76 中的恒等式加以适当的变形，以构造一个其左端是 $2(p-1)$ 次多项式，其右端是 $3(p-1)$ 次多项式的恒等式.

85. 若想利用问题 76 的论证来证明

$$[f(x,y,z)]^{p-1}\equiv 1-(1-x^{p-1})(1-y^{p-1})(1-z^{p-1}) \pmod p$$

对一切 x,y,z 成立，多项式函数 $f(x,y,z)$ 需要具备什么条件?

86. 如果 $[f(x,y,z)]^{p-1}\equiv 1-(1-x^{p-1})(1-y^{p-1})(1-z^{p-1})$ $\pmod p$，那么对多项式函数 f 的次数加上什么样的限制条件就会导致与问题81矛盾的结果?

87. 证明: 每一个最高次数 $<n$ 而且常数项为零的整系数多项式 $f(x_1,x_2,\cdots,x_n)$ 必有非平凡解 $\pmod p$[1] (Chevalley 定理).

注记与答案

参考书见书目:

Ore (1948), Shanks (1978), Davenport (1968).

1. $18-(-14)=32\equiv 0 \pmod 4$.

$$b=a+4n,\quad d=c+4m.$$

因此

$$bd=(a+4n)(c+4m)=ac+4(am+nc+4mn)$$
$$\equiv ac \pmod 4.$$

[1] 即 $f(x_1,x_2,\cdots,x_n)\equiv 0 \pmod p$ 有解 $(x_1^0,x_2^0,\cdots,x_n^0)\not\equiv(0,0,\cdots,0) \pmod p$.——译者注.

2.

×	−4	5	2	−1
−4	−4	−4	−4	−4
5	−−4	5	2	−1
2	−4	2	−4	2
−1	−4	−1	2	5

3. $a-b=hn$, $c-d=kn$.

因此

$ac-bd=hnc+bkn=n(hc+bk)\equiv 0 \pmod{n}$.

4. $a_i a_j$ 只属于一个剩余类，因此与唯一的 a_k 同余.

若 $a_Z \equiv 0 \pmod{n}$，则 $a_Z a_i \equiv 0 \equiv a_Z \pmod{n}$.

若 $a_I \equiv 1 \pmod{n}$，则 $a_I a_i \equiv a_i \pmod{n}$.

5. 每个 a_i 都有唯一的 b_j 与它同余；由此推出的结构的相似性已在问题 3 中证明.

6. 是的: 1.

7, 8, 9, 10 从第二列开始，这些表给出了数列的前 $n-1$ 项.

11. $0 \equiv na \pmod{n}$，见问题 2.36.

12. 4, 6, 8, 9, 10, 12, 14, 15, 16.

13. 若 $n=hk$，则位在第 $(h+1)$ 行与第 $(k+1)$ 列的数是 0.

因为每行含 n 个数，所以有两个零的行少一个 Z_n 的元素.

14. 若 p 是素数，则对于所有的 $a \not\equiv 0 \pmod{p}$，有 $\gcd(a, p)=1$. 由问题 2.38 知，数列 $a, 2a, 3a, \cdots$ 在第 $p+1$ 项之前无重复. 这样，表中含 a 的行有 p 个不同的数，所以它含有 Z_p 的全部元素. 因此 $x \to ax$ 是 Z_p 的一个置换. 在 Z_p 中,仅当 $x=y$，即 $x \equiv y \pmod{p}$ 时，才有 $ax=ay$. 另一个证明方法: $ax \equiv ay \pmod{p} \Rightarrow a(x-y) \equiv 0 \pmod{p} \Rightarrow p \mid a$ 或 $p \mid (x-y)$. 此外，若 $x \to ax$ 是 Z_p 的一个置换，则对于任意的 $b \in Z_p$，都存在唯一的 x，使得 $ax=b$.

15. 在映射 $x\to ax$ 之下，$0\to 0$，所以 $x\to ax$ 是 Z_p 中非零元素的一个置换．于是 $\{1,2,\cdots,p-1\}\equiv\{a,2a,\cdots,(p-1)a\}\pmod p$，而且

$$1\cdot 2\cdots(p-1)\equiv a\cdot 2a\cdots(p-1)a \pmod p.$$

像问题 14 中那样相约，得到 $1\equiv a^{p-1}\pmod p$．

16. 令 $b=1$ 或利用 $a^{p-2}a\equiv 1\pmod p$．

17. 若 p 不是 a，b 或 ab 的因数，则集合是封闭的；单位元素是 1；在问题 16 中已证明了存在逆元素．在乘法运算下，由模 p 的全体非零剩余构成的群，可以表示为定义了模 p 乘法的一个完全剩余系（其中去掉了与 0 同余的元素），也可以表示为：取全体非零剩余类作为元素，以及利用通常的整数乘法来定义它的乘法．

这个群的存在性是本章其余部分的基础．在问题 61 中将证明，这个群一定是循环群．

18. Z_p 的非零元素构成一个 $p-1$ 阶的群．由 Lagrange 定理知道，元素的阶整除群的阶，所以必有某个 $d\mid p-1$ 使在这个群中有 $x^d=1$ 成立．于是 $x^{p-1}=x^{d(p-1)/d}=1^{p-1/d}=1$．

19. 若 $x\not\equiv 0\pmod p$，则 $x^{p-1}\equiv 1\Rightarrow x^p\equiv x$．

若 $x\equiv 0\pmod p$，则 $x^p\equiv 0\equiv x$．

问题 15，18，19 的结果应该记住．以后随时要用到．

20. $2222\equiv 3\pmod 7$，$5555\equiv 4\pmod 7$，$5555\equiv 5\pmod 6$，$2222\equiv 2\pmod 6$．$2222^{5555}+5555^{2222}\equiv 3^5+4^2\equiv 12+2\equiv 0\pmod 7$．

21. ± 1．若 $x^2-1\equiv 0\pmod p$，则 $p\mid x-1$ 或 $p\mid x+1$．

22. $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6=(2\cdot 4)(3\cdot 5)6\equiv 6\pmod 7$．

23. $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10$

$=(2\cdot 6)(3\cdot 4)(5\cdot 9)(7\cdot 8)10\equiv 10\equiv -1\pmod{11}$．

24. 凡不满足 $x^2=1$ 的都是.

25. $(p-1)!\equiv -1 \pmod{p}$.

我们在这里证明 Wilson 定理，对它的实质比对它的应用更为重视.

26. 6,13; 没有; 仅有 8.

27. (i) 0,2,4,6,8,10,12.

(ii) 1,3,5,7,9,11,13.

28. $4x\equiv b \pmod{14} \Rightarrow b=4x+14k$，所以 b 是偶数.

29. $2c=4x+14k \Longleftrightarrow c=2x+7k \Longleftrightarrow 2x\equiv c \pmod{7}$. 但 $2\cdot 4\equiv 1 \pmod{7}$，所在 $2x\equiv c \pmod{7} \Longleftrightarrow x\equiv 4c \pmod{7}$. 在 14 个数 $4c, 4c+1, \cdots, 4c+13$ 中，只有 $4c$ 和 $4c+7$ 与 $4c$ 同余 $\pmod{7}$.

30. $ax\equiv b \pmod{n} \Rightarrow b=ax+kn \Rightarrow \gcd(a, n) \mid b$.

31. $ar+ns=1 \Rightarrow arb+nsb=b \Rightarrow arb\equiv b \pmod{n}$，所以 $ax\equiv b \pmod{n}$ 有一个解.

32. $ax\equiv b \pmod{n}$ 和 $ay\equiv b \pmod{n} \Rightarrow ax\equiv ay \pmod{n}$，所以 $n \mid a(x-y)$. 但是 $\gcd(a, n)=1$，所以 $n \mid x-y$，即 $x\equiv y \pmod{n}$.

33. 若 $\gcd(a,n)=d$，则 $\gcd\left(\frac{a}{d}, \frac{n}{d}\right)=1$. 由 $ax\equiv b \pmod{n} \Rightarrow b=ax+kn$，又由 $d\mid b \Rightarrow \frac{b}{d}=\frac{a}{d}x+k\frac{n}{d}$，这是一个整系数方程. 所以 $\frac{a}{d}x\equiv\frac{b}{d} \pmod{\frac{n}{d}}$，而由问题 31 知它有一个解，再由问题 32 可知它的解在 $0\leqslant x<\frac{n}{d}$ 中是唯一的. 若 r 是这个解，那么在数 $r, r+1, \cdots, r+(n-1)$ 中，只有形如 $r+k\frac{n}{d}$ 的那些数与 r 同余 $\pmod{\frac{n}{d}}$. 所以当 $k=0, 1, \cdots, d-1$ 时，就得到 $ax\equiv b \pmod{n}$ 的不同的解.

事实上，凡满足 $ax \equiv b \pmod{n}$ 的整数 x 必满足 $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$，反过来也对.

34. $a=1,3,5,9,11,13$.

若 $x \to ax$ 是一个置换，则对某个 x，有 $ax \equiv 1$.

若 $ax \equiv 1$，则 $a(xb) \equiv b$，因此 $x \to ax$ 是一个满射.

35. $a=1,5,7,11$.

36. (ii)与(iii)的等价性已在注记34中证明.

利用 $\gcd(a,n)=1 \Longleftrightarrow$ 存在整数 x,y，使得 $ax+ny=1 \Longleftrightarrow ax \equiv 1 \pmod{n}$.

我们证明了(i)与(ii)的等价性.

由(i)可知，一个简化剩余系中含有 $\varphi(n)$ 个元素.

M_n 还可以定义为由 $(Z_n,+)$ 的生成元所组成的集合.

37. $\gcd(a,p)=1 \Longleftrightarrow a \not\equiv 0 \pmod{p}$.

这一点很重要：要灵活地把 M_n 看成是定义了模 n 乘法的简化剩余系，或者看成是定义了像在问题3中那样自然地引进的乘法的相应的剩余类集合.

38.

1	3
3	1

1	5
5	1

1	3	5	7
3	1	7	5
5	7	1	3
7	5	3	1

1	3	7	9
3	9	1	7
7	1	9	3
9	7	3	1

1	2	4	5	7	8
2	4	8	1	5	7
4	8	7	2	1	5
5	1	2	7	8	4
7	5	1	8	4	2
8	7	5	4	2	1

39. 是.

40. 显然 $1 \in M_n$. 因为 $ab \cdot 1 \Rightarrow ba \equiv 1$, 所以 M_n 的每个元素有一个逆元素. 若 $ab \equiv 1$ 及 $cd \equiv 1$, 则 $(ac)(bd) \equiv 1$, 所以 M_n 是封闭的.

41. 因为 M_n 是一个群, $x \to ax$ 是 M_n 的一个置换, 所以 $\{a_1, \cdots, a_{\varphi(n)}\} \equiv \{a_i a_1, \cdots, a_i a_{\varphi(n)}\} \pmod{n}$. 于是 $a_1 \cdots a_{\varphi(n)} \equiv a_i a_1 \cdots a_i a_{\varphi(n)} \pmod{n}$. 两边相约可得 $1 = (a_i)^{\varphi(n)} \pmod{n}$.

42. 因为 M_n 是一个 $\varphi(n)$ 阶的群, 所以每个元素的阶整除 $\varphi(n)$. 从而对于 $a \in M_n$, $a^{\varphi(n)} = 1$ 成立.

43. (i) 7, 22; (ii) 没有; (iii) 7; (iv) 4.

44. 由 $\gcd(a_1, m_1) = \gcd(a_2, m_2) = 1$ 及问题 31 与问题32 可知,每个方程都有唯一解.利用孙子定理及 $\gcd(m_1, m_2) = 1$ 可知联立方程有唯一解.

45. 当 $n = 8, 12, 15$ 或 16 时, $x^2 = 1$ 有四个解. 当 n 是合数时, 虽然 $x^2 \equiv 1 \pmod{n} \Rightarrow n \mid (x+1)(x-1)$, 但却不一定有 $n \mid x+1$ 或 $n \mid x-1$.

46. mod 5; 1. mod 7; 1, 2, 4. mod 11; 1. mod 13; 1, 3, 9.

$(x-1)(x-2)(x-4) \equiv x^3 - 1 \pmod{7}$,

$(x-1)(x-3)(x-9) \equiv x^3 - 1 \pmod{13}$.

$x^3 - 1 = (x-1)(x^2+x+1)$, 所以 $x^2+x+1 \equiv 0$ 的解必定是 $x^3 - 1 \equiv 0$ 的解.

47. 由 Fermat 定理得到: mod 5; 1, 2, 3, 4. mod 7; 1, 6. mod 11; 1, 10. mod 13; 1, 5, 8, 12.

$(x-1)(x-2)(x-3)(x-4) \equiv x^4 - 1 \pmod{5}$,

$(x-1)(x-5)(x-8)(x-12) \equiv x^4 - 1 \pmod{13}$.

$x^4 - 1 = (x-1)(x+1)(x^2+1)$, 所以 $x^2 + 1 \equiv 0$ 的解必定是 $x^4 - 1 \equiv 0$ 的解.

48. mod 7; 1. mod 11; 1, 3, 4, 5, 9. mod 13; 1.

$(x-1)(x-3)(x-4)(x-5)(x-9) \equiv (x^5-1) \pmod{11}$.
$x^5-1=(x-1)(x^4+x^3+x^2+x+1)$，所以$x^4+x^3+x^2+x+1\equiv 0$的解必定是$x^5-1\equiv 0$的解.

49. $g(x)=x^{n-1}+x^{n-2}+\cdots+x+1$.

50. $g(x)=x^{n-1}+ax^{n-2}+\cdots+a^i x^{n-i-1}+\cdots+a^{n-1}$.

51. 若$f(x)=b_n x^n+b_{n-1}x^{n-1}+\cdots+b_0$，则

$f(x)-f(a)=b_n(x^n-a^n)+b_{n-1}(x^{n-1}-a^{n-1})+\cdots+b_1(x-a)$.
由问题 50可知每一项都有因式$x-a$，所以

$$f(x)-f(a)=(x-a)g(x),$$

而且当$f(a)=0$时，有$f(x)=(x-a)g(x)$.

如果$f(a)\equiv 0 \pmod p$，那么由$f(x)=(x-a)g(x)+f(a)$.
又推出$f(x)\equiv(x-a)g(x) \pmod p$.

52. 选取k使得x^5项的系数为零.

选取l使得x^4项的系数为零.

选取m使得x^3项的系数为零.

选取n使得x^2项的系数为零.

选取p使得x项的系数为零.

选取q使得常数项为-1.

53. $x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-(p-1)) \pmod p$.
当p是奇素数时，$p-1$是偶数，上式右端常数项为$(p-1)!$. 当$p=2$时，Wilson 定理是显然的.

54. 令$x^3-1=(x-a)(x-b)(x-c)+k(x-a)(x-b)+l(x-a)+m$.
因为$a^3-1\equiv 0 \pmod{19}$，所以$m=0 \pmod{19}$.

因为$b^3-1\equiv 0 \pmod{19}$，$b\not\equiv a \pmod{19}$，所以$l\equiv 0 \pmod{19}$.

因为$c^3-1\equiv 0 \pmod{19}$，$c\not\equiv a,b \pmod{19}$，所以$k\equiv 0 \pmod{19}$.

因此$x^3-1\equiv(x-a)(x-b)(x-c) \pmod{19}$.

现在$0\equiv d^3-1\equiv(d-a)(d-b)(d-c) \pmod{19}$. 但

这将导致 $d\equiv a$, b 或 c (mod 19).

55. 在上题注记中以 p 代替 19.

56. 恰好 n 个. 证明与注记 54 类似.

57. 若 $b_1, \cdots, b_n$ 是不同的零点, 利用问题 52 的方法可以证明

$$a_0x^n+\cdots+a_n=a_0(x-b_1)\cdots(x-b_n).$$

这样, 左端多项式的另外一个零点至少应该是右端一个因式的零点. 无论我们是在全体整数中考虑, 还是对素数模来考虑, 这个结论总是对的; 在后一种情形, 必须有 $a_0\not\equiv 0 \pmod{p}$.

58.

mod 3	元素	1	2										
	阶	1	2										
mod 5	元素	1	2	3	4								
	阶	1	4	4	2								
mod 7	元素	1	2	3	4	5	6						
	阶	1	3	6	3	6	2						
mod 11	元素	1	2	3	4	5	6	7	8	9	10		
	阶	1	10	5	5	5	10	10	10	5	2		
mod 13	元素	1	2	3	4	5	6	7	8	9	10	11	12
	阶	1	12	3	6	4	12	12	4	3	6	12	2

此处, 群的阶分别是 2, 4, 6, 10, 12. 在每个群中都找到了生成元, 所以它们是循环群.

59. 由 Lagrange 定理知 $d|p-1$.

$1, a, a^2, \cdots, a^{d-1}$ 是不同的解. 由问题 57 的 Lagrange 定理知道它们就是全部解. 因此每个 d 阶元素都属于这个集合. 但是这些 d 阶元素恰好是这个群的生成元, 所以共有 $\varphi(d)$ 个 d 阶元素.

60. $N_d=0$ 或 $N_d=\varphi(d)$.

若 d 不是 $p-1$ 的因数, 则根据关于子群的 Lagrange 定理, 可知 M_p 不含 d 阶元素.

61．每个元素有一个阶，所以必被计算一次．所有的阶都是$p-1$的约数．由于$N_{d_i}\leqslant\varphi(d_i)$而且两个和数相同，所以对于每个约数$d_i$，$N_{d_i}=\varphi(d_i)$．

62．当$n=4,6,9,10,14$时是循环群．至此，我们已经证明当n是素数及$n=4,6,9,10,14$时，存在原根．

63．每一列是模3的完全剩余系，每一行是模4的完全剩余系．这些删除达到简化的目的．对于模12，我们有$\{1,5\}\cdot\{1,7\}=\{1,5,7,11\}$，即$M_3\cdot M_4=M_{12}$．

64．

mod 36	1	29	13	5	25	17	mod 9
	19	11	31	23	7	35	
mod 4							

$19\cdot25\equiv1\cdot7\equiv7\pmod 9$；$19\cdot25\equiv3\cdot1\pmod 4$．由孙子定理知道，只有一个数$\pmod{36}$同于余$7\pmod 9$和同余于$3\pmod 4$．7就是这样一个数．

$\{1,29,13,5,25,17\}$是模9的一个简化剩余系，且每个元素都$\equiv1\pmod 4$．因此，它是与M_9同构的M_{36}的子群．同样地，$\{1,19\}$是模4的一个简化剩余系，每个元素都$\equiv1\pmod 9$．因此，它是与M_4同构的M_{36}的子群．

65．由问题2.50知，删去不与mn互素的数后，余下的阵列有$\varphi(m)$行，$\varphi(n)$列．含有1的那一行是模n的一个简化剩余系，它的元素都$\equiv1\pmod m$，所以这一行是与M_n同构的M_{mn}的子群．同样地，含有1的那一列是与M_m同构的M_{mn}的子群．如果$b\equiv1\pmod n$，则$ab\equiv a\pmod n$，于是a和ab属于同一列．如果$a\equiv1\pmod m$，则$ab\equiv b\pmod m$，于是b和ab属于同一行．这样，这个阵列就具体地表示出了直积$M_{mn}=M_m\cdot M_n$．

66．在M_{63}中，$\{1,10,19,37,46,55\}=M_7$及$\{1,8,22,29,43,50\}=M_9$．方阵中异于1的元素在M_{63}中的阶都是3．

1	37	46
22	58	4
43	16	25

这是两个3阶群的直积．

67．若n是奇数，则$\gcd(2,n)=1$，于是$M_{2n}=M_2\cdot M_n$，但$M_2=\{1\}$．

68．mod 9；2，$2^5=5$．mod 27；2，$2^5=5$，$2^7=20$，$2^{11}=23$，$2^{13}=11$，$2^{17}=14$．mod 81；2，$2^5=32$，$2^7=47$，$2^{11}=23$，$2^{13}=11$，$2^{17}=14$，$2^{19}=56$，$2^{23}=5$，$2^{25}=20$，$2^{29}=77$，$2^{31}=65$，$2^{35}=68$，$2^{37}=29$，$2^{41}=59$，$2^{43}=74$，$2^{47}=50$，$2^{49}=38$，$2^{53}=41$．

69．$(3k+1)^3=27k^3+27k^2+9k+1\equiv 1\pmod 9$，

$(3k+1)^9=(9h+1)^3=9^3h^3+3\cdot 9^2h^2+27h+1\equiv 1\pmod{27}$，

$(3k+1)^{27}=(27g+1)^3=27^3g^3+3\cdot 27^2g^2+81g+1\equiv 1\pmod{81}$．

若$(3k+1)^{3^{n-1}}\equiv 1\pmod{3^n}$，则$(3k+1)^{3^n}=(3^nh+1)^3\equiv 1\pmod{3^{n+1}}$．

70．(i) 利用问题3．

(ii) 根据(i)的意义．

(iii) $(pk+a)^{dp}=(1+hp)^p\equiv 1\pmod{p^2}$．

(iv) $(pk+a)^{dp^2}=(1+gp^2)^p\equiv 1\pmod{p^3}$．

因此，$pk+a$对模p^2的阶不是$p(p-1)$，对模p^3的阶不是$p^2(p-1)$．

71．此时$3k+2$的阶是1，2或3，但不是6．$(3k+2)^3\equiv 2^3\pmod 3$．$2^3\not\equiv 1\pmod 3$．因此$3k+2$不是3阶$\pmod 9$．若$(3k+2)^2\not\equiv 1\pmod 9$，则$3k+2$的阶不是1或2，于是由这个条件推出$3k+2$的阶为6．

$9k^2+12k+4\not\equiv 1\pmod 9\Leftrightarrow 3k+3\not\equiv 0\pmod 9$

$\Leftrightarrow k+1\not\equiv 0\pmod 3\Leftrightarrow k\equiv 0,1\pmod 3$．

72．模p^2原根的阶是$p(p-1)$．给出的每个条件都与此矛

盾. 如果两个条件都不成立，则$pk+a$的阶不可能是$p(p-1)$的真因子.

$$(pk+a)^{pd} \equiv (pk+a)^{d} \pmod p \quad (\text{由 Fermat 定理})$$
$$\equiv a^{d} \pmod p$$
$$\not\equiv 1 \pmod p \quad (\text{因为 } a \text{ 是原根而且 } d<p-1).$$

选取k,使得$h-a^{p-2}k \not\equiv 0 \pmod p$.

73. $(pk+a)^{p-1}=1+pu \Rightarrow (pk+a)^{p(p-1)}=(1+pu)^{p}$

$$=1+p^{2}u+p^{3}(\cdots).$$

当$d<p-1$时，又有$(pk+a)^{dp^{2}} \equiv a^{d} \not\equiv 1 \pmod p$.

74. 模p^{n}原根的阶与模$2p^{n}$原根的阶都是$p^{n-1}(p-1)$. 因此，若$a+kp^{n}$是奇数，则它必属于$M_{2p^{n}}$，而且它的阶就是原根的阶.

75. $(1,1,1) \pmod 3$, $(0,1,2) \pmod 5$, $(1,2,3) \pmod 7$.

76. 由假设及 Fermat 定理知道，除$x \equiv y \equiv z \equiv 0$外，左端$\equiv 1$. 若$x,y,z$中有一个$\not\equiv 0$，则由 Fermat 定理知道，$(1-x^{p-1})(1-y^{p-1})(1-z^{p-1}) \equiv 0$.

77. $2(p-1)$； $x^{p-1}y^{p-1}z^{p-1}$的次数为$3(p-1)$.

78. $x^{p} \equiv x \pmod p$，所以$x^{p+n} \equiv x^{1+n} \pmod p$.

79. 如果$f(x)-g(x) \equiv 0 \pmod p$对不同余的整数都成立，由于$f(x)-g(x)$的次数$\leqslant p-1$，这就和 Lagrange 定理（问题57）矛盾. 因此$f(x)-g(x)$一定是一个零多项式$\pmod p$①，从而f与g中x的相同次项的系数对模p同余.

80. 将$f(x,y)$与$g(x,y)$看作是x的多项式，并设在f与g中x^{i}的系数分别是$a_{f}(y)$与$a_{g}(y)$. 那么由上题知，对于所有的整数y有$a_{f}(y) \equiv a_{g}(y)$，再应用上题的结果，就可推出a_{f}与a_{g}中y的相同次项的系数对 mod p 是同余的.

---

① 若多项式的系数都是同余于0模p，则称它是零多项式$\pmod p$.

——译者注.

81．将$f(x,y,z)$与$g(x,y,z)$看作是z的多项式，然后利用问题 79 和问题 80．

82．右端的$x^{p-1}y^{p-1}z^{p-1}$的系数是1，而左端是 0，但是由问题 81 知，它们却应该对模p同余．

83．$(xyz+x^2+y^2+z^2)^{p-1}\equiv 1-(1-x^{p-1})(1-y^{p-1})(1-z^{p-1})$. 左边和右边的$x^{p-1}y^{p-1}z^{p-1}$项的系数都是 1．

84．$(x^2+y^2+z^2-3)^{p-1}$
$\equiv 1-[1-(x-1)^{p-1}][1-(y-1)^{p-1}][1-(z-1)^{p-1}]$．

85．仅当$x\equiv y\equiv z\equiv 0$时，$f(x,y,z)\equiv 0 \pmod p$．

86．$f(x,y,z)$的最大次数 <3．

87．若$f(x_1,\cdots,x_n)\equiv 0$仅有解$x_1\equiv x_2\equiv\cdots\equiv x_n\equiv 0 \pmod p$，则$[f(x_1,\cdots,x_n)]^{p-1}\equiv 1-(1-x_1^{p-1})\cdots(1-x_n^{p-1})$.

若f的最高次数小于n，则与问题 81 推广到n个变量所得的结果矛盾．

历史注记

1640 年，Fermat 在一封信中提出了他的定理．在 1773 年，J. L. Lagrange 首先发表了 Fermat 定理的证明，过去曾把此归功于 Wilson，时间大约还要早三年．Euler 对 Fermat 定理的推广是 1760 年发表的．利用 Lagrange 关于多项式的工作，A．M．Legender 在 1785 年在理论上给出了模p的原根的构造．C．F．Gauss 在 1801 年证明了只有模 2，4，p^n和$2p^n$才有原根．用商环的单位群的语言讨论这些性质是二十世纪的事．我们所说的 Chevalley 定理是 C．Chevalley 在 1936 年所发表的某项工作的一个简化情形．

本书前三章中绝大部分结果的详细介绍，可参见 Ore 的书(1948)．

第四章　二次剩余

二次剩余与 Legendre 符号

1. 在 Z_7 中，分别求出方程 $x^2=0,1,2,3,4,5,6$ 的所有解.

2. 在 Z_7 中，方程

(i) $(x+2)^2=0$,　(v) $x^2+2x=3$,　(ix) $x^2+3x=3$,
(ii) $(x+2)^2=1$,　(vi) $x^2+2x=4$,　(x) $x^2+3x=4$,
(iii) $(x+2)^2=2$,　(vii) $x^2+2x=5$,　(xi) $x^2+3x=5$,
(iv) $(x+2)^2=3$,　(viii) $x^2+2x=6$,　(xii) $x^2+3x=6$,

当中，哪些无解，哪些有一个解，哪些有两个解？

3. M_7 中的完全平方数称为对模7的二次剩余. 写出由 $x\to x^2$ 给出的 M_7 的映射结果. 在这个映射下，全体像的集合是否构成 M_7 的子群?

4. 利用表 3.2，求出对模5，模11，模12以及模13的二次剩余. 对于哪些模，全体二次剩余构成 M_n 的子群? 对于 n 的哪些数值，映射 $x\to x^2$ 使 M_n 的两个元素对应同一个元素?

5. 对于模3，5，7，11，13及17，分别说出二次剩余的个数. 试预言对模 p (是奇素数)的二次剩余的个数.

6. 若 p 是素数，由 $x^2\equiv y^2 \pmod p$ 能否断定 $x\equiv y \pmod p$ 或 $x\equiv -y \pmod p$?

7. 对于任意的素数 p，求 M_p 中被 $x\to x^2$ 映射成1的那些元素. 你能说出，在这个映射下，M_p 中有多少个元素被映射成任何另外的二次剩余吗?

8. M_n中不是平方的数称为对模n的二次非剩余[1]. 求三个对模n的二次非剩余.

9. 求所有的对模7的二次剩余的三次方，以及所有的对模7的二次非剩余的三次方.

10. 对于方程$x^6 \equiv 1 \pmod 7$的解的个数，从Fermat定理能得出什么结论?

关于对模7的二次剩余的三次方，你能推出什么结论?

将x^6-1分解因式并利用Lagrange定理 (问题3.57)，证明同余于$1 \pmod 7$的立方数至多有三个. 同余于$-1 \pmod 7$的立方数也至多有三个.

11. 利用上题的方法，求同余于$1 \pmod{11}$的五次方数的个数，以及同余于$-1 \pmod{11}$的五次方数的个数. 从五次方数的值能不能决定这个数是不是二次剩余?

12. 推广问题10和问题11的方法，给出一个准则，用它能判定哪些数是对模p的二次剩余，哪些数是对模p的二次非剩余 (p是奇素数).

13. 利用$(xy)^k=x^ky^k$，证明M_n中的k次幂数的集合构成一个子群.

14. 设p是奇素数，那么M_p在映射$x \to x^{\frac{1}{2}(p-1)}$下的像是什么?

15. 通常用Legendre符号$\left(\frac{a}{p}\right)$ (有时记作$(a|p)$)表示: $+1$，当a是对模p的二次剩余；-1，当a是对模p的二次非剩余；以及0，其他情形. 证明

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

16. 写出不超过20的素数，使得对于等于这个素数的模，

(i) -1是二次剩余，

(ii) -1是二次非剩余.

---

[1] 一般地，也称为"模n的二次非剩余"，或"二次非剩余, mod n". —— 译者注.

能否看出其中的规律?

17. 作为群 M_p 中的元素, -1 的阶是多少? M_p 中有没有另外的元素与 -1 有相同的阶?

18. 设 p 是奇素数,

(i) 若 $(-1)^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$,

(ii) 若 $(-1)^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$,

那么, 对于 p 你能说些什么?

19. 设 p 是奇素数, M_p 中由二次剩余构成的子群的阶是什么? p 为何值时, 这个阶是偶数? p 为何值时, 这个阶是奇数?

20. 奇数阶的群为什么不含有 2 阶元素?

21. 通过将元素与它的逆元素配对, 证明偶数阶的群必定含有 2 阶元素.

22. 若 p 是 $4k+1$ 形的素数, M_p 是否必有 4 阶元素?

23. 求 2^2+1, 3^2+1, 4^2+1, 5^2+1, 6^2+1, 7^2+1, 8^2+1 以及 9^2+1 的奇素因数.

其中形如 $4k+1$ 与 $4k+3$ 的素因数各有多少个?

24. 设 p 是奇素数而且整除形如 n^2+1 的某数. 你能否证明 p 具有 $4k+1$ 的形式?

25. 将问题 1.65 中的方法做些变化, 证明存在无限多个形如 $4k+1$ 的素数.

26. 求 2^2+2+1, 3^2+3+1, 4^2+4+1, 5^2+5+1, 6^2+6+1, 7^2+7+1, 8^2+8+1 以及 9^2+9+1 的素因数.

其中形如 $3k+1$ 的素因数有多少个?

27. 设 p 是奇素数而且整除形如 n^2+n+1 的某个数, 证明: $p=3$, 或者 p 具有 $3k+1$ 的形式 (因为 M_p 含有 3 阶元素).

28. 将问题 25 中的方法做些变化, 证明存在无限多个形如 $3k+1$ 的素数.

29. 设 p 是形如 $4k+1$ 的素数, 用 Wilson 定理 (问题 3.25)

证明

$$(1\cdot 2\cdot 3\cdots 2k)^2\equiv -1 \pmod p.$$

Gauss 引理

下面的十三个问题将逐步地建立起一个判断一个数是不是对模p的二次剩余的方法．

30．在表4.1中，利用绝对最小剩余系给出了M_3，M_5，M_7，M_{11}和M_{13}的乘法表．

如果仅考虑绝对值，说明为什么每个表的第一行的前一半和后一半恰好次序相反．为什么这些表的每一列也是如此？证明所有可能取到的绝对值都出现在每行的前半部分．

表 4.1

模3的绝对最小剩余的乘法

1	−1
−1	1

模5的绝对最小剩余的乘法

1	2	−2	−1
2	−1	1	−2
−2	1	−1	2
−1	−2	2	1

模7的绝对最小剩余的乘法

1	2	3	−3	−2	−1
2	−3	−1	1	3	−2
3	−1	2	−2	1	−3
−3	1	−2	2	−1	3
−2	3	1	−1	−3	2
−1	−2	−3	3	2	1

模 11 的绝对最小剩余的乘法

1	2	3	4	5	−5	−4	−3	−2	−1
2	4	−5	−3	−1	1	3	5	−4	−2
3	−5	−2	1	4	−4	−1	2	5	−3
4	−3	1	5	−2	2	−5	−1	3	−4
5	−1	4	−2	3	−3	2	−4	1	−5
−5	1	−4	2	−3	3	−2	4	−1	5
−4	3	−1	−5	2	−2	5	1	−3	4
−3	5	2	−1	−4	4	1	−2	−5	3
−2	−4	5	3	1	−1	−3	−5	4	2
−1	−2	−3	−4	−5	5	4	3	2	1

模 13 的绝对最小剩余的乘法

1	2	3	4	5	6	−6	−5	−4	−3	−2	−1
2	4	6	−5	−3	−1	1	3	5	−6	−4	−2
3	6	−4	−1	2	5	−5	−2	1	4	−6	−3
4	−5	−1	3	−6	−2	2	6	−3	1	5	−4
5	−3	2	−6	−1	4	−4	1	6	−2	3	−5
6	−1	5	−2	4	−3	3	−4	2	−5	1	−6
−6	1	−5	2	−4	3	−3	4	−2	5	−1	6
−5	3	−2	6	1	−4	4	−1	−6	2	−3	5
−4	5	1	−3	6	2	−2	−6	3	−1	−5	4
−3	−6	4	1	−2	−5	5	2	−1	−4	6	3
−2	−4	−6	5	3	1	−1	−3	−5	6	4	2
−1	−2	−3	−4	−5	−6	6	5	4	3	2	1

31. 在表 4.1 中，计算每一行的前半部分中负号的个数．对于$p=3, 5, 7, 11, 13$，将每个 M_p 的元素列成表，并且把与每个元素相对应的负号个数的奇偶性标上去．将这个表与二次剩余和二次非剩余的表做比较．

32. 将以下各数

$2\cdot1, 2\cdot2, 2\cdot3, 2\cdot4, 2\cdot5, 2\cdot6, 2\cdot7, 2\cdot8$

都表示成绝对最小剩余 (mod 17)，即表示成 $+8$ 与 -8 之间的一个数．证明 $2^8\equiv(-1)^4\equiv1 \pmod{17}$．利用问题 12 判

断 2 是不是对模 17 的二次剩余．

33．对于模 17，有

$3\cdot1\equiv3$，　$3\cdot2\equiv6$，$3\cdot3\equiv-8$，$3\cdot4\equiv-5$，

$3\cdot5\equiv-2$，　$3\cdot6\equiv1$，$3\cdot7\equiv4$，　$3\cdot8\equiv7$．

证明 $3^8\equiv-1\ (\mathrm{mod}\ 17)$，并且判断 3 是不是对模 17 的二次剩余．

34．用问题 32 的方法判断 2 是不是对模 19 的二次剩余．

35．设 a 是 M_{17} 的一个元素，证明分别与

$a\cdot1$，$a\cdot2$，$a\cdot3$，$a\cdot4$，$a\cdot5$，$a\cdot6$，$a\cdot7$，$a\cdot8$

$(\mathrm{mod}\ 17)$ 同余的绝对最小剩余的绝对值都不同．说明怎样计算 $a^8\ (\mathrm{mod}\ 17)$，以及怎样判定 a 是不是二次剩余．

36．设 p 是奇素数，证明分别同余于

$$2\cdot1,2\cdot2,2\cdot3,\cdots,2\cdot\frac{1}{2}(p-1)$$

$(\mathrm{mod}\ p)$的绝对最小剩余的绝对值都不相同．如何计算 $2^{\frac{1}{2}(p-1)}$ $(\mathrm{mod}\ p)$?

37．利用上题证明，若 $p=8k+1$，则 2 是对模 p 的二次剩余．

38．利用问题 36 证明，如果 $p=8k+3$，则 2 是对模 p 的二次非剩余．

39．利用问题 36，确定 2 是不是对模 $p=8k+5$ 的二次剩余．

40．利用问题36，确定 2 是不是对模 $p=8k+7$ 的二次剩余．

41．当 $p=8k+1$，$8k+3$，$8k+5$，$8k+7$ 时，判断 $\frac{1}{8}(p^2-1)$ 的奇偶性并且证明 $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$．

这个结果的形式虽然很怪，却是判定二次剩余的一个基本结论．因为这个结果不容易记住，所以你要记着在哪里能查到它．

42．当 $p=8k+1$，$8k+3$，$8k+5$，$8k+7$ 时，计算 $\left(\frac{-2}{p}\right)$ 的值．

43. 设 p 是奇素数，a 是 M_p 的元素，证明：分别同余于

$$a \cdot 1, a \cdot 2, a \cdot 3, \cdots, a \cdot \frac{1}{2}(p-1)$$

$(\bmod\ p)$ 的绝对最小剩余的绝对值都不相同．若在这些数中有 l 个取负号，则 $a^{\frac{1}{2}(p-1)} = (-1)^l$ (Gauss 引理)．

二次互反律

下一个问题引进了一个新记号．

44. 记 $[\frac{7}{2}] = 3, [3] = 3, [\sqrt{2}] = 1, [0.9] = 0, [-\frac{1}{2}] = -1$．一般地，对于实数 x，$[x]$ 是一个整数，$[x] \leqslant x < [x] + 1$，称 $[x]$ 为 x 的整数部分．

求 $\frac{11}{13} - [\frac{11}{13}]$，$\frac{22}{13} - [\frac{22}{13}]$，$\frac{33}{13} - [\frac{33}{13}]$，$\frac{44}{13} - [\frac{44}{13}]$，$\frac{55}{13} - [\frac{55}{13}]$，$\frac{66}{13} - [\frac{66}{13}]$，其中有几个超过 $\frac{1}{2}$？

45. 若同余于 $x\ (\bmod\ 13)$ 的绝对最小剩余是负的，关于 $\frac{x}{13} - [\frac{x}{13}]$ 的值能说些什么？

若同余于 $x\ (\bmod\ 13)$ 的绝对最小剩余是正的，关于 $\frac{x}{13} - [\frac{x}{13}]$ 的值能说些什么？

46. 利用问题 43－45，判断 11 是不是对模 13 的二次剩余，并用表 3.2 检验你的答案．

47. 用间隔至少一公分的方格纸，或者用类似的有格点的纸，标出点

$(1, \frac{11}{13})$, $(2, \frac{22}{13})$, $(3, \frac{33}{13})$, $(4, \frac{44}{13})$, $(5, \frac{55}{13})$, $(6, \frac{66}{13})$，以及

$(1, [\frac{11}{13}])$, $(2, [\frac{22}{13}])$, $(3, [\frac{33}{13}])$, $(4, [\frac{44}{13}])$, $(5, [\frac{55}{13}])$, $(6, [\frac{66}{13}])$.

48. 我们把两个坐标都是整数的点称为格点. 在三条线段

$$y=\frac{11}{13}x, y=\frac{11}{13}x+\frac{1}{2}, y=\frac{11}{13}x-\frac{1}{2} \ (0<x<13)$$

上，是否有格点？

49. 在线段 $y=\frac{11}{13}x-\frac{1}{2}$ 与 $y=\frac{11}{13}x+\frac{1}{2}$ $(1\leqslant x\leqslant 6)$ 之间有多少个格点？

50. 利用问题 47 (必要时，为了精确些，可以利用问题 44 的计算)，确定在线段 $y=\frac{11}{13}x$ 与 $y=\frac{11}{13}x+\frac{1}{2}$ $(1\leqslant x\leqslant 6)$ 之间的格点数目. 分别同余于11, 22, 33, 44, 55, 66 (mod 13) 的绝对最小剩余中，带负号的数的个数和这个格点数目有什么关系？能从这个数目确定11是不是对模13的二次剩余吗？

51. 将 $\frac{13}{11}-[\frac{13}{11}]$, $\frac{26}{11}-[\frac{26}{11}]$, $\frac{39}{11}-[\frac{39}{11}]$, $\frac{52}{11}-[\frac{52}{11}]$ 及 $\frac{65}{11}-[\frac{65}{11}]$ 表示成简分数，其中有几个大于 $\frac{1}{2}$？若 $\frac{x}{11}-[\frac{x}{11}]$ 大于 $\frac{1}{2}$，那么关于 x 的绝对最小剩

余 (mod 11)能说些什么？

利用这些结论来判定 13 是不是对模 11 的二次剩余，并用表 3.2 检验你的结论．

52．在问题 47 中所用的那种方格纸上，标出点 $(\frac{13}{11}, 1)$, $(\frac{26}{11}, 2)$, $(\frac{39}{11}, 3)$, $(\frac{52}{11}, 4)$, $(\frac{65}{11}, 5)$，以及 $([\frac{13}{11}], 1)$, $([\frac{26}{11}], 2)$, $([\frac{39}{11}], 3)$, $([\frac{52}{11}], 4)$, $([\frac{65}{11}], 5)$．

53．在线段

$$x=\frac{13}{11}y,\ x=\frac{13}{11}y-\frac{1}{2},\ x=\frac{13}{11}y+\frac{1}{2}\quad(0<y<1).$$

上有没有格点？

54．在线段

$$x=\frac{13}{11}y-\frac{1}{2}\ \text{与}\ x=\frac{13}{11}y+\frac{1}{2}\quad(1\leqslant y\leqslant 5)$$

之间有多少个格点？

55．利用问题 52 (必要时，为了精确些，可以利用问题 51 的计算)，确定在线段 $x=\frac{13}{11}y$ 与 $x=\frac{13}{11}y+\frac{1}{2}$ $(1\leqslant y\leqslant 5)$ 之间的格点的数目．怎样利用这个数判断 13 是不是对模 11 的二次剩余？

56．画出矩形 $1\leqslant x\leqslant 6$, $1\leqslant y\leqslant 5$ 并大略地标明直线 $y=\frac{11}{13}x+\frac{1}{2}$, $y=\frac{11}{13}x$，以及 $x=\frac{13}{11}y+\frac{1}{2}$ 与矩形的关系．有多少个格点在这个矩形的内部和周界上？在以$(3\frac{1}{2}, 3)$

为中心旋转半周所成的映射（即$(x,y)\to(-x+7,-y+6)$）下，矩形与直线$y=\frac{11}{13}x+\frac{1}{2}$的像是什么？

57. 证明矩形$1\leqslant x\leqslant 6$，$1\leqslant y\leqslant 5$内的格点数的奇偶性和在矩形内且界于直线$y=\frac{11}{13}x+\frac{1}{2}$与$x=\frac{13}{11}y+\frac{1}{2}$之间的格点数的奇偶性相同.

58. 设p与q是不同的奇素数，在线段$y=\frac{p}{q}x$与$y=\frac{p}{q}x+\frac{1}{2}$ $(1\leqslant x\leqslant\frac{q-1}{2})$之间的格点个数为$l$. 用Gauss引理来说明为什么$(\frac{p}{q})=(-1)^l$.

59. 设p,q是奇素数，而且在线段$x=\frac{q}{p}y$与$x=\frac{q}{p}y+\frac{1}{2}$ $(1\leqslant y\leqslant\frac{p-1}{2})$之间的格点数为$m$. 说明为什么$(\frac{q}{p})=(-1)^m$. 证明$(\frac{p}{q})(\frac{q}{p})=(-1)^{m+l}$.

60. 证明：在对于点$(\frac{1}{4}(q+1),\frac{1}{4}(p+1))$旋转半周所成的映射（即$(x,y)\to(-x+\frac{1}{2}(q+1),-y+\frac{1}{2}(p+1))$）下，矩形$1\leqslant x\leqslant\frac{1}{2}(q-1)$，$1\leqslant y\leqslant\frac{1}{2}(p-1)$映射到自身，以及直线$y=\frac{p}{q}x+\frac{1}{2}$与$x=\frac{q}{p}y+\frac{1}{2}$互映到对方. 证明：

$l+m$（定义见问题58与问题59）与 $\frac{1}{4}(p-1)(q-1)$ 有相同的奇偶性，因此 $(-1)^{l+m}=(-1)^{\frac{1}{4}(p-1)(q-1)}$.

61. 利用表3.2，求：$(\frac{3}{5})$ 与 $(\frac{5}{3})$，$(\frac{3}{7})$ 与 $(\frac{7}{3})$，$(\frac{5}{7})$ 与 $(\frac{7}{5})$，$(\frac{3}{11})$ 与 $(\frac{11}{3})$，$(\frac{5}{11})$ 与 $(\frac{11}{5})$，$(\frac{7}{11})$ 与 $(\frac{11}{7})$，$(\frac{3}{13})$ 与 $(\frac{13}{3})$，$(\frac{5}{13})$ 与 $(\frac{13}{5})$，$(\frac{7}{13})$ 与 $(\frac{13}{7})$.

分出 $(\frac{p}{q})\neq(\frac{q}{p})$ 的那些情形.

62. 利用问题60明确地判定，什么时候有 $(\frac{p}{q})\neq(\frac{q}{p})$？

（二次互反律）

63. 证明下面推理的每个步骤的合理性：

$$\left(\frac{350}{19}\right)=\left(\frac{2\cdot5\cdot5\cdot7}{19}\right)$$

$$=\left(\frac{2}{19}\right)\left(\frac{5}{19}\right)\left(\frac{5}{19}\right)\left(\frac{7}{19}\right)$$

$$=\left(\frac{2}{19}\right)\left(\frac{7}{19}\right)$$

$$=-\left(\frac{7}{19}\right)$$

$$= \left(\frac{19}{7}\right)$$

$$= \left(\frac{5}{7}\right)$$

$$= \left(\frac{7}{5}\right)$$

$$= \left(\frac{2}{5}\right)$$

$$= -1.$$

64. 按照$p \equiv 1, 5, 7, 11 \pmod{12}$分别求出$\left(\frac{3}{p}\right)$.

65. 按照 $p \equiv 1, 3, 7, 9 \pmod{10}$分别求出$\left(\frac{5}{p}\right)$.

注记与答案

参考书见书目：Shanks (1978)， Davenport (1968)，Bolker (1970).

1. $0^2=0, 1^2=6^2=1, 3^2=4^2=2, 2^2=5^2=4$. 使用等号"="而不是同余号"≡"，是为了表明我们把模 7 的七个剩余类看成是 Z_7 的元素.

2. 无解： (iv)，(vi)，(vii)，(xii).
   一个解：(i)， (viii)，(ix).
   二个解：(ii)，(iii)， (v)， (x)， (xi).

3.

1	2	3	4	5	6	子群	1	4	2
1	4	2	2	4	1		4	2	1
							2	1	4

M_n 中的完全平方数称为对模 n 的二次剩余.

4. 全是子群.

	1	4	模 5				1	模 12					
	4	1											

1	4	9	5	3	模 11	1	4	9	3	12	10	模 13
4	5	3	9	1		4	3	10	12	9	1	
9	3	4	1	5		9	10	3	1	4	12	
5	9	1	3	4		3	12	1	9	10	4	
3	1	5	4	9		12	9	4	10	1	3	
						10	1	12	4	3	9	

两个对应一个：5，11，13

四个对应一个：12.

5. 1，2，3，5，6，8. $\frac{1}{2}(p-1)$.

6. $x^2 \equiv y^2 \Rightarrow x^2 - y^2 \equiv 0 \Rightarrow (x+y)(x-y) \equiv 0 \pmod{p}$

$\Rightarrow p \mid x+y$ 或 $p \mid x-y$.

7. $x^2 \equiv 1 \pmod{p} \Rightarrow p \mid x+1$ 或 $p \mid x-1 \Rightarrow x \equiv \pm 1 \pmod{p}$.

由问题 6 可知，恰好有两个.

8. 5，7，11.

9. $(\text{q.r.})^3 \equiv 1 \pmod{7}$，$(\text{q.n-r.})^3 \equiv -1 \pmod{7}$[1].

10. 在 M_7 中恰有六个根.

对于所有的 $x \in M_7$，有 $(x^2)^3 \equiv 1 \pmod{7}$，因此三个二次剩余都是方程 $x^3 \equiv 1$ 的解. $x^6 - 1 = (x^3-1)(x^3+1)$.

---

[1] "q.r."与"q.n-r."分别是"二次剩余"与"二次非剩余"的缩写.

——译者注.

由 Lagrange 定理知道，$x^3 \equiv -1$ 恰好有三个解，所以它们都是二次非剩余．

11．由 Fermat 定理知，$x^{10}-1 \equiv 0 \pmod{11}$有十个解．五个二次剩余满足 $x^5 \equiv 1$．$x^{10}-1=(x^5-1)(x^5+1)$．$x^5 \equiv -1$ 恰有五个解，它们一定是二次非剩余．

12．由 Fermat 定理知，$x^{p-1} \equiv 0 \pmod{p}$有$p-1$个根．根据问题 6，有 $\frac{1}{2}(p-1)$个二次剩余，它们满足 $x^{\frac{1}{2}(p-1)}-1 \equiv 0 \pmod{p}$．因为 $x^{p-1}-1=(x^{\frac{1}{2}(p-1)}-1)\cdot(x^{\frac{1}{2}(p-1)}+1)$，所以由 Lagrange 定理可知$x^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$恰有 $\frac{1}{2}(p-1)$个根，它们一定就是所有的二次非剩余．

13．由 $x^k y^k=(xy)^k$得出封闭性．$1^k=1$．

若 $ax \equiv 1$，则 $(ax)^k \equiv 1$，所以 $a^k x^k \equiv 1$，从而每个k 次幂的逆元素仍是一个 k 次幂．

特别地，我们证明了,M_n 中的二次剩余构成一个子群．

14．$\{1, -1\}$．

15．若 $a \equiv 0 \pmod{p}$，则 $ab \equiv 0 \pmod{p}$，而且

$$\left(\frac{ab}{p}\right)=0=0\cdot\left(\frac{b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

若 $a \not\equiv 0 \pmod{p}$，则$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$（问题 12）．因此，若 $a, b \not\equiv 0 \pmod{p}$，则

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{1}{2}(p-1)}=a^{\frac{1}{2}(p-1)}b^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

在 Legendre 符号的定义中，p 是奇素数．若 p 不一定是素数，则可定义一个具有某些相同性质的类似的符号，它称为 Jacobi 符号．

16. -1是对下列各个模的二次剩余:5，13，17 $\equiv 1 \pmod 4$

-1 是对于下列各个模的二次非剩余:3,7,11,19$\equiv 3 \pmod 4$.

17. 两个．由问题 7 知，没有另外的 2 阶元素．

18. (i) $\frac{1}{2}(p-1)$一定是偶数,所以$4 \mid p-1$，$p\equiv 1 \pmod 4$.

(ii) $\frac{1}{2}(p-1)$一定是奇数，所以 $p-1=2(2k+1)$，$p\equiv 3 \pmod 4$．

19. 由二次剩余构成的子群的阶是$\frac{1}{2}(p-1)$．当$p\equiv 1 \pmod 4$时，阶是偶数；$p\equiv 3 \pmod 4$时，阶是奇数．

20. 元素的阶整除群的阶．

21. 除1 阶与 2 阶元素外，其他元素与自已的逆元素都不相同．因此，在一个群中，阶不是1 和 2 阶的元素有偶数个．如果群的阶是偶数，那么它的 1 阶和 2 阶元素有偶数个．但是，1 是唯一的 1 阶元素，所以至少有一个 2 阶元素．

22. 若$p=4k+1$，则由二次剩余构成的群的阶是 $2k$．因为阶是偶数，所以这个群含有一个 2 阶元素．但是只有 -1 是 2 阶的，所以 -1 是二次剩余，从而对于某个 a 有 $a^2\equiv -1 \pmod p$成立．元素 a 在 M_p 中是 4 阶．

另解：若 b 为二次非剩余,则由问题 12 知道 $b^{2k}\equiv -1 \pmod p$.因此 b^k 的阶不是 1 或 2．然而由Fermat 定理知，$b^{4k}\equiv 1 \pmod p$，所以 b^k 的阶是 4．

23. 5，5，17，13，37，5，5 及 13，41．它们都同余于 $1 \pmod 4$．

24. 若$p \mid n^2+1$，则$n^2\equiv -1 \pmod p$，于是 -1 是二次剩余．由问题 18 与问题 12 可知$p\equiv 1 \pmod 4$．

25. 使用问题 1.64 中的记号，$p_1^2p_2^2p_3^2\cdots p_n^2+1$ 不能被任何 $\leqslant p_n$ 的素数整除，所以它的素因数大于 p_n. 再由问题 24 知它的素因数都是 $4k+1$ 的形式. 所以这种形式的素数个数无限.

26. $7, 13, 3\cdot 7, 31, 43, 3\cdot 19, 73, 7\cdot 13$.

除 3 以外都是 $3k+1$ 的形式.

27. 若 $p\mid n^2+n+1$，则 $p\mid n^3-1=(n-1)(n^2+n+1)$，因此 n 在 M_p 中是 1 阶或 3 阶. 若 n 是 1 阶，则 $p=3$. 若 n 是 3 阶，那么 M_p 含有 3 阶元素，所以 $3\mid p-1$，$p\equiv 1 \pmod 3$.

28. 使用问题 1.64 中的记号，令 $m=p_1p_2\cdots p_n$，则 $m(m+1)+1$ 没有 $\leqslant p_n$ 的素因数，所以它的素因数大于 p_n. 由问题 27 知，它的素因数都是 $3k+1$ 的形式，所以这种形式的素数个数无限.

29. 由 Wilson 定理知 $1\cdot 2\cdots 4k\equiv -1 \pmod p$. 但是 $2k+1\equiv -2k, \cdots, -2\equiv 4k-1, -1\equiv 4k$，所以

$1\cdot 2\cdots 2k\cdot(-2k)\cdots(-2)(-1)\equiv -1 \pmod p$,

其中有 $2k$ 个负号. 因此

$$(1\cdot 2\cdots 2k)^2\equiv -1 \pmod p.$$

这证明了 $1\cdot 2\cdots 2k$ 是 M_p 中的 4 阶元素.

在以下十三个问题中，需要记住的结论是：对于奇素数 p，-1 是对模 $p\equiv 1 \pmod 4$ 的二次剩余，也是对模 $p\equiv 3 \pmod 4$ 的二次非剩余. 这个结果将在第六章用到.

30. 每行含有偶数 $(p-1)$ 个元素. $p-1\equiv -1, p-2\equiv -2, \cdots, p-\frac{1}{2}(p-1)\equiv -\frac{1}{2}(p-1)$，所以第一行的后一半按绝对值重复了前一半. 在下面的行里，前一半中的每个元素 ab 与后一半中的 $a(-b)=-(ab)$ 对应. $x\longrightarrow ax$ 是 M_p 的一个置换，因而每个绝对值必定恰也出现二次，所以前一半包含了所有可能的绝对值，且仅取一次.

31.

	偶	奇
mod 3	1	-1
mod 5	$1, -1$	$2, -2$
mod 7	$1, 2, -3$	$3, -2, -1$
mod 11	$1, 3, 4, 5, -2$	$2, -5, -4, -3, -1$
mod 13	$1, 3, 4, -4, -3, -1$	$2, 5, 6, -2, -5, -6$
	二次剩余	二次非剩余

32. $2, 4, 6, 8, -7, -5, -3, -1$.

因此,$2^8(1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8) \equiv (-1)^4(1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8) \pmod{17}$. 因为 $2^8 \equiv (-1)^4 \equiv 1 \pmod{17}$,所以2是 二次剩余.

33. $3^8(1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8)$

$\equiv (-1)^3(1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8) \pmod{17}$.

所以 $3^8 \equiv (-1)^3 \equiv -1 \pmod{17}$, 因而3是二次非剩余.

34. $2\cdot1 \equiv 2, 2\cdot2 \equiv 4, 2\cdot3 \equiv 6, 2\cdot4 \equiv 8, 2\cdot5 \equiv -9, 2\cdot6 \equiv -7, 2\cdot7 \equiv -5, 2\cdot8 \equiv -3, 2\cdot9 \equiv -1 \pmod{19}$.
因此 $2^9(1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9) \equiv (-1)^5(1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9) \pmod{19}$. 因为 $2^9 \equiv -1 \pmod{19}$,所以2是二次非剩余.

35. 在问题30中已经证明了有不同的绝对值.设这些绝对最小剩余中有m个是负的,则

$a^8 \equiv (1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8) \equiv (-1)^m(1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8) \pmod{17}$,于是 $a^8 \equiv (-1)^m \pmod{17}$. 若$m$是偶数,则$a^8 \equiv 1$, a是二次剩余. 若m是奇数,则 $a^8 \equiv -1$, a是二次非剩余.

36. 绝对值不相同的证明类似于问题30.

设在这些绝对最小剩余中有m个是负的,则 $2^{\frac{1}{2}(p-1)} \equiv (-1)^m \pmod{p}$. 因此, 2是或不是二次剩余由$m$是偶数或是奇数而定.

37. 若$p = 8k+1$,则绝对最小剩余在 $\pm 4k$ 之间.

$2\cdot1, 2\cdot2, \cdots, 2\cdot4k \equiv 2, 4, \cdots, 4k, -4k+1, -4k+3, \cdots, -3, -1$.

这些绝对最小剩余中恰好有$2k$个是负的,所以$2^{4k} \equiv (-1)^{2k} \equiv 1$

(mod p), 2 是二次非剩余.

38. 若 $p=8k+3$, 则绝对最小剩余在 $\pm(4k+1)$ 之间.

$2\cdot1,\cdots,2(4k+1)\equiv2,4,\cdots4k,-4k-1,-4k+1,\cdots,-3,-1.$

这些绝对最小剩余中恰好有 $2k+1$ 个是负的, 所以 $2^{4k+1}\equiv(-1)^{2k+1}$ $\equiv-1 \pmod p$, 2 是二次非剩余.

39. 若 $p=8k+5$, 则绝对最小剩余在 $\pm(4k+2)$ 之间.

$2\cdot1,\cdots,2(4k+2)\equiv2,4,\cdots,4k+2,-4k-1,-4k+1,\cdots,-3,-1.$

这些绝对最小剩余中恰好有 $2k+1$ 个是负的, 所以

$2^{4k+2}\equiv(-1)^{2k+1}\equiv-1 \pmod p$, 2 是二次非剩余.

40. 若 $p=8k+7$, 则绝对最小剩余在 $\pm(4k+3)$ 之间.

$2\cdot1,\cdots,2(4k+3)\equiv2,4,\cdots,4k+2,-4k-3,-4k-1,-4k+1,\cdots,-3,-1.$

这些绝对最小剩余中恰好有 $2k+2$ 个是负的, 所以

$2^{4k+3}\equiv(-1)^{2k+2}\equiv1 \pmod p$, 2 是二次剩余.

41. 若 $p=8k+1$, $(p-1)(p+1)=8k(8k+2)$, 于是 $\frac{1}{8}(p^2-1)=2k(4k+1)$, 偶数.

若 $p=8k+3$, $(p-1)(p+1)=(8k+2)(8k+4)$, $\frac{1}{8}(p^2-1)=(4k+1)(2k+1)$, 奇数.

若 $p=8k+5$, $(p-1)(p+1)=(8k+4)(8k+6)$, $\frac{1}{8}(p^2-1)=(2k+1)(4k+3)$, 奇数.

若 $p=8k+7$, $(p-1)(p+1)=(8k+6)(8k+8)$, $\frac{1}{8}(p^2-1)=2(4k+3)(k+1)$, 偶数.

由问题 37—40 推出所要证明的结论.

42.

	$p=8k+1$	$8k+3$	$8k+5$	$8k+7$
	$\left(\frac{-1}{p}\right)=1$	-1	1	-1
	$\left(\frac{2}{p}\right)=1$	-1	-1	1
所以	$\left(\frac{-2}{p}\right)=1$	1	-1	-1

43. 由问题 30 知道 绝对值各不相同, 于是

$$a^{\frac{1}{2}(p-1)}\left[1\cdot2\cdot3\cdots\frac{1}{2}(p-1)\right]\equiv(-1)^l\left[1\cdot2\cdots\frac{1}{2}(p-1)\right]$$

$(\bmod p)$, $a^{\frac{1}{2}(p-1)} \equiv (-1)^l (\bmod\ p)$. 所以当 l 是偶数时，a 是二次剩余，当 l 是奇数时，a 是二次非剩余.

44. $\frac{11}{13}$，$\frac{9}{13}$，$\frac{7}{13}$，$\frac{5}{13}$，$\frac{3}{13}$，$\frac{1}{13}$. 前三个大于 $\frac{1}{2}$.

45. 若 $x \equiv a\ (\bmod\ 13)$ 且 $-6 \leqslant a \leqslant -1$，则 $x-a \equiv 0\ (\bmod\ 13)$，而且 $\frac{x-a}{13}$ 是大于 $\frac{x}{13}$ 的整数.

所以 $\frac{x}{31}-[\frac{x}{13}]=\frac{x}{13}-(\frac{x-a}{13}-1)=\frac{a}{13}+1>\frac{1}{2}$.

若 $x \equiv a\ (\bmod\ 13)$ 且 $1 \leqslant a \leqslant 6$，则 $\frac{x-a}{13}$ 是小于 $\frac{x}{13}$ 的整数，所以 $\frac{x}{13}-[\frac{x}{13}]=\frac{x}{13}-\frac{x-a}{13}=\frac{a}{13}<\frac{1}{2}$.

46. 因为 $\frac{11}{13}$，$\frac{9}{13}$，$\frac{7}{13}>\frac{1}{2}$，所以由问题 44 和问题45 知道，与 11，22，33 同余的绝对最小剩余是负的，与 44，55，66 同余的则是正的. 这样，由问题 43 知，$11^6 \equiv (-1)^3\ (\bmod\ 13)$，所以 11 是对模 13 的二次非剩余.

48. 在直线 $y=\frac{11}{13}x$ 上，$x=1,2,\cdots,12$ 时 $y=\frac{11}{13},\frac{22}{13},\cdots,\frac{132}{13}$. 因为 13 不能整除 $11x$，所以这些数都不是整数也不是整数 $\pm\frac{1}{2}$.

49. 六个，因为这两条线段沿 y 方向的距离是 1.

50. 三个. 对于给定的 x，在直线 $y=\frac{11}{13}x$ 与 $y=\frac{11}{13}x+\frac{1}{2}$ 之间，或者在 $y=\frac{11}{13}x$ 与 $y=\frac{11}{13}x-\frac{1}{2}$ 之间有一个格点，但不会同时有格点. 当 $\frac{11}{13}x-[\frac{11}{13}x]<\frac{1}{2}$ 时，第二对直线间有格点；当 $\frac{11}{13}x-[\frac{11}{13}x]>\frac{1}{2}$ 时，第一对直线间有格点，在同余于 $11x$

(mod 13)的绝对最小剩余是负数时出现这种情形.

51. $\frac{2}{11}$, $\frac{4}{11}$, $\frac{6}{11}$, $\frac{8}{11}$, $\frac{10}{11}$. 后面的三个 $>\frac{1}{2}$.

$$1>\frac{x}{11}-[\frac{x}{11}]>\frac{1}{2}\Leftrightarrow 0>\frac{x}{11}-[\frac{x}{11}+1]>-\frac{1}{2}$$

$$\Leftrightarrow 0>x-11[\frac{x}{11}+1]>-\frac{11}{2}.$$

因此,同余于 x (mod 11)的绝对最小剩余是负数. 这样,同余于 39, 52 及 65 (mod 11)的绝对最小剩余都是负数. 根据 Gauss 引理, 13是对模 11 的二次非剩余.

53. 没有.

54. 五个,因为这两条线段沿 x 方向的距离是 1.

55. 利用与问题 50 相似的推理可知有三个. 而由问题 51 知道, 这些格点的 y 坐标使得同余于 $13y$ (mod 11)的绝对最小剩余是负的. 所以,根据 Gauss 引理,13 是对模 11的二次非剩余.

56. 在矩形上有三十个格点(见图 4.1). $(3\frac{1}{2}, 3)$是矩形中心. 方程$y=\frac{11}{13}x+\frac{1}{2}$ 与$(-x+7)=\frac{13}{11}(-y+6)+\frac{1}{2}$ 等价. 因此,当且仅当点$(-x+7, -y+6)$在直线 $x=\frac{13}{11}y+\frac{1}{2}$ 上时,

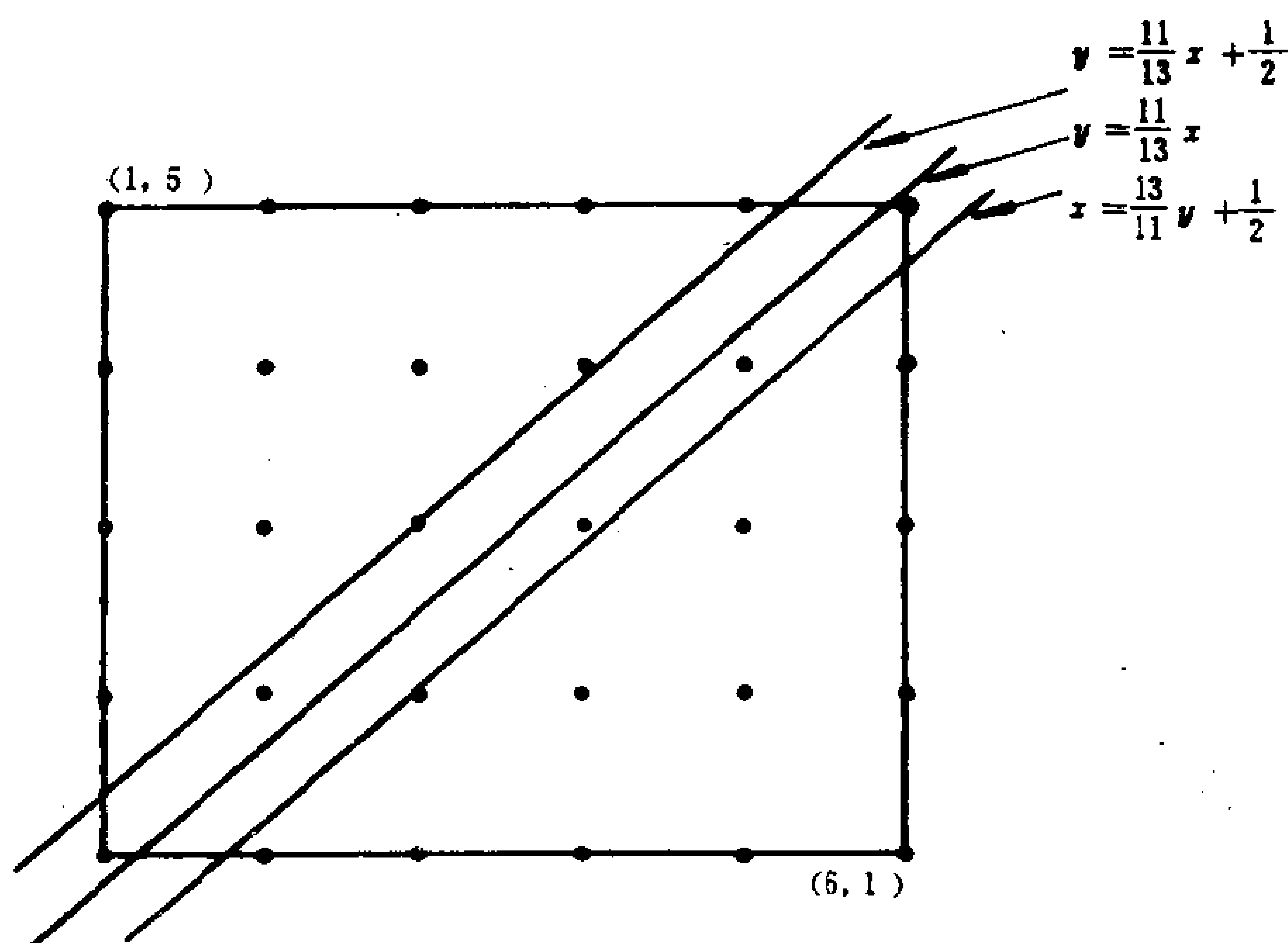


图 4.1

点(x,y)在直线$y=\frac{11}{13}x+\frac{1}{2}$上，而且，在旋转半周的映射下，这个矩形的像是它自身，这两条直线则互为映像.

57. 在问题56中的旋转半周所成的映射下，A与B互为映像，因而它们含有相同的格点数.

在A和B中的格点数$\equiv 0 \pmod{2}$.

在A和B和C中的格点数$\equiv$ C中的格点数$\pmod{2}$. 在本题中，我们有$30\equiv 6 \pmod{2}$. （见图4.2).

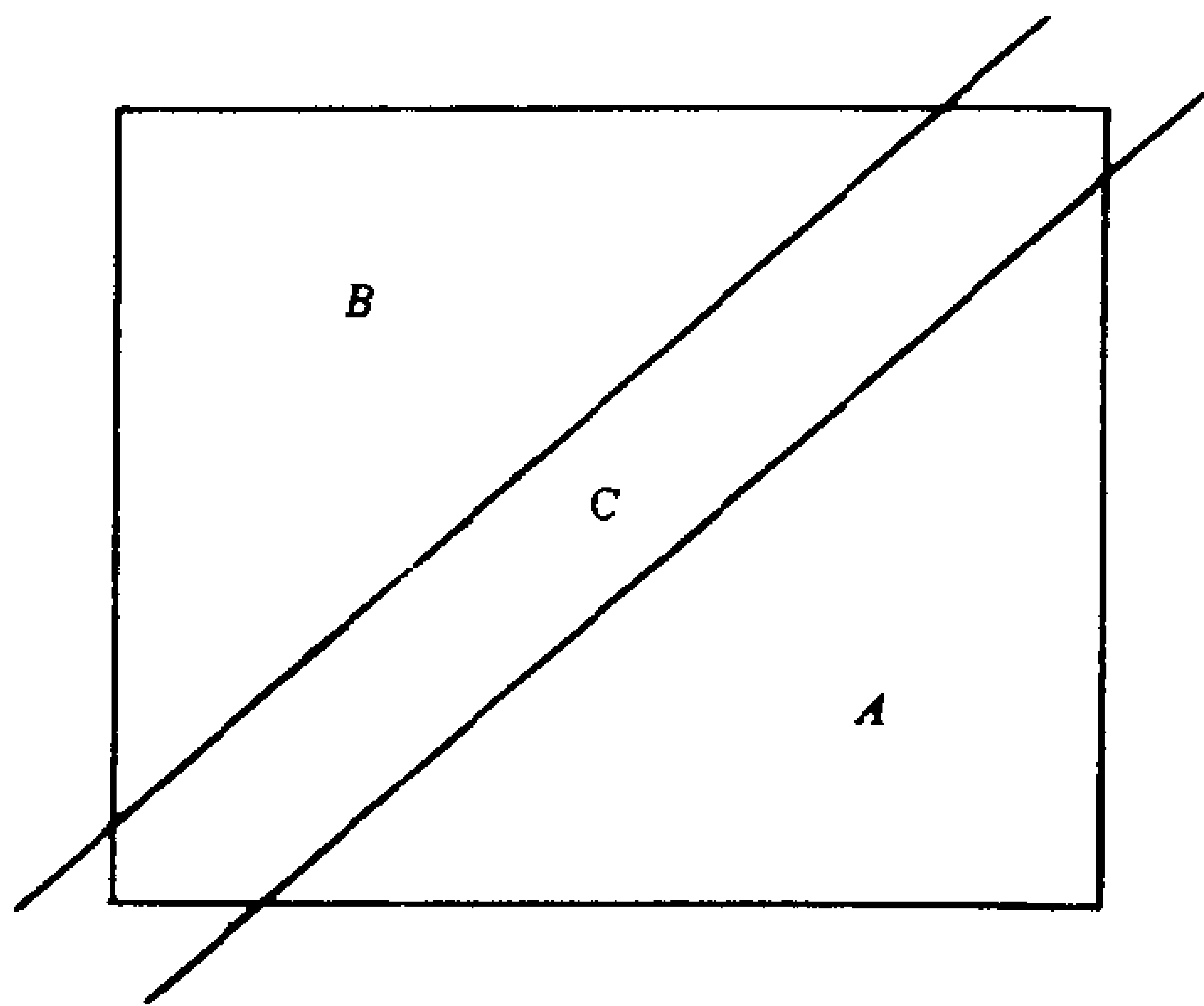


图 4.2

58. 对给定的整数x，当$\frac{p}{q}x-[\frac{p}{q}x]>\frac{1}{2}$时，在$y=\frac{p}{q}x$与$y=\frac{p}{q}x+\frac{1}{2}$之间有一个格点. 当$1\leqslant x\leqslant q-1$时，由于$p$和$q$是不同的奇素数，所以在这些直线上没有格点. 推广问题45的论证得出：仅当同余于$px \pmod{q}$的绝对最小剩余是负数时，$\frac{p}{q}x-[\frac{p}{q}x]>\frac{1}{2}$. 因此，如果在区域中有$l$个格点，那么根据Gauss引理，$(\frac{p}{q})=(-1)^l$.

59．类似上题推出$(\frac{q}{p})=(-1)^m$，于是$(\frac{p}{q})(\frac{q}{p})=(-1)^{l+m}$．

60．从问题57中的图看出，C含有$l+m$个格点，整个矩形含有$\frac{1}{4}(p-1)(q-1)$个格点．因为A和B含有相同数目的格点，所以$l+m\equiv\frac{1}{4}(p-1)(q-1)\pmod 2$．

61．-1与-1，-1与1，-1与-1，1与-1，1与1，-1与1，1与1，-1与-1，-1与-1．

$(\frac{3}{7})\neq(\frac{7}{3})$，$(\frac{3}{11})\neq(\frac{11}{3})$，$(\frac{7}{11})\neq(\frac{11}{7})$．

62．除$\frac{1}{4}(p-1)(q-1)$是奇数外，$(\frac{p}{q})=(\frac{q}{p})$．

若$p=4k+1$，则$\frac{1}{4}(p-1)(q-1)=k(q-1)$是偶数．

若$p=4k+3$且$q=4h+3$，则

$\frac{1}{4}(p-1)(q-1)=(2k+1)(2h+1)$是奇数．

因此，除$p\equiv q\equiv 3\pmod 4$外，$(\frac{p}{q})=(\frac{q}{p})$．

63．(i)分解350，(ii)根据问题15，(iii)$(\frac{a^2}{19})=1$，(iv)$(\frac{2}{19})=-1$(问题38)，(v)二次互反律，(vi)$19\equiv 5\pmod 7$，(vii)二次互反律，(viii)$7\equiv 2\pmod 5$，(ix)$(\frac{2}{5})\equiv -1$(问题39)．

64．$(\frac{3}{12k+1})=(\frac{12k+1}{3})=(\frac{1}{3})=1$．

$$\left(\frac{3}{12k+5}\right)=\left(\frac{12k+5}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

$$\left(\frac{3}{12k+7}\right)=-\left(\frac{12k+7}{3}\right)=-\left(\frac{1}{3}\right)=-1.$$

$$\left(\frac{3}{12k+11}\right)=-\left(\frac{12k+11}{3}\right)=-\left(\frac{2}{3}\right)=1.$$

65. $$\left(\frac{5}{10k+1}\right)=\left(\frac{10k+1}{5}\right)=\left(\frac{1}{5}\right)=1.$$

$$\left(\frac{5}{10k+3}\right)=\left(\frac{10k+3}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

$$\left(\frac{5}{10k+7}\right)=\left(\frac{10k+7}{5}\right)=\left(\frac{2}{5}\right)=-1.$$

$$\left(\frac{5}{10k+9}\right)=\left(\frac{10k+9}{5}\right)=\left(\frac{4}{5}\right)=\left(\frac{2^2}{5}\right)=1.$$

历史注记

虽说 Euler 和 Lagrange 都知道二次互反律，而且 Legendre 还用它来研究二次型，但是二次互反律的第一个证明是Gauss，是在 1801 年给出的．Gauss 在他的一生中还给出了好几个不同的证明，其中的几个证明可见 Mathews 的书 (日期不详)．

第五章　方程$x^n+y^n=z^n$ $(n=2,3,4)$

方程　$x^2+y^2=z^2$

1. 表5.1是一个平方和表.利用左边的一列平方数,找出表中所有的平方数.表中大于2500的平方数只有2704.

2. 表5.1中,在通过0与$4^2+3^2=5^2$的直线上,哪些数是平方数？找出这些数中的第一个数后,你能预先说出其他数吗?

3. 在通过0与$12^2+5^2=13^2$的直线上的平方数是哪些?它们之间有何相似之处?

4. 利用$24^2+7^2=25^2$及$15^2+8^2=17^2$,再指出表5.1中的两个平方数.

5. 若x,y,z是使$x^2+y^2=z^2$成立的正整数,则称(x,y,z)是一个Pythagoras三元数组.此外,若$\gcd(x,y,z)=1$,则称(x,y,z)为本原Pythagoras三元数组.从表5.1中可找出七个本原Pythagoras三元数组(把(x,y,z)与(y,x,z)看做是相同的).

6. 设(x,y,z)是一个Pythagoras三元数组,判断下述情况是否可能,并说明理由:

(i) x,y,z全是偶数,

(ii) x,y,z中只有两个是偶数,

(iii) x,y,z中只有一个是偶数,

(iv) x,y,z都不是偶数.

7. 设(x,y,z)是一个Pythagoras三元数组,判断下述情况是否可能,并说明理由:

(i) x,y,z都被3整除,

(ii) x, y, z中只有两个被 3 整除,

(iii) x,y,z 中只有一个被 3 整除,

(iv) x,y,z 都不被 3 整除.

为做第(iv)小题,要列出一个 $\mathbf{Z}_3$ 中的平方和表.

8. 设(x,y,z)是一个Pythagoras 三元数组,判断下述情况是否可能,并说明理由:

(i) x,y,z 都被 5 整除,

(ii) x,y,z 中只有两个被 5 整除,

(iii) x,y,z 中只有一个被 5 整除,

(iv) x,y,z 都不被 5 整除.

为做第(iv)小题,要列出一个 $\mathbf{Z}_5$ 中的平方和表.

9. 设(x,y,z)是一个 Pythagoras 三元数组,通过列出 $\mathbf{Z}_4$ 中的平方和表来证明:仅当 x 与 y 都是偶数时,z 才是偶数. 设 x 是偶数、但 y,z 都是奇数,利用 $x^2=z^2-y^2$ 证明 x 有因数 4.

10. 设(x, y, z)是一个 Pythagoras 三元数组, $\sin\theta=\frac{x}{z}$, $\operatorname{tg}\theta=\frac{x}{y}$ (见图 5.1). 利用 $x:y:z=2\operatorname{tg}\frac{\theta}{2}:(1-\operatorname{tg}^2\frac{\theta}{2}):(1+\operatorname{tg}^2\frac{\theta}{2})$证明 $\operatorname{tg}\frac{\theta}{2}=\frac{x}{y+z}$.

设 $\operatorname{tg}\frac{\theta}{2}=\frac{q}{p}$,其中 p 与 q 是整数且$\gcd(p,q)=1$,证明 $x:y:z=2pq:(p^2-q^2):(p^2+q^2)$.

11. 对于任意的正整数 $p,q,p>q$,证明$(2pq,p^2-q^2,p^2+q^2)$是 Pythagoras 三元数组.

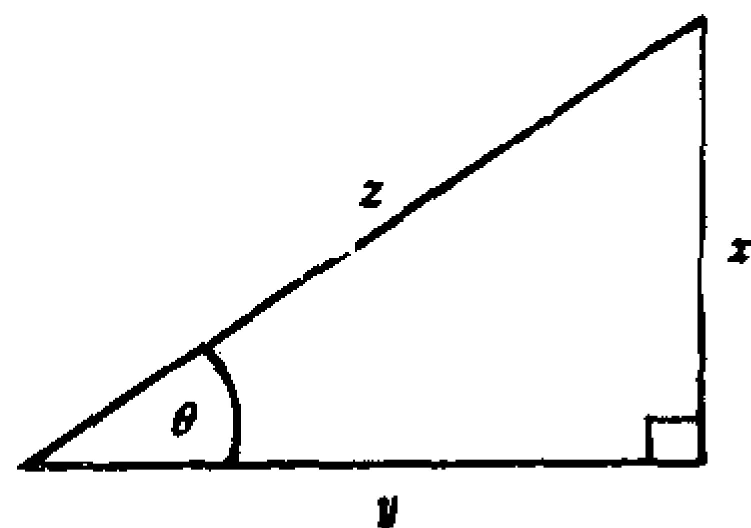


图 5.1

12. 求正整数 p,q,使得 $2pq=4$, $p^2-q^2=3$ 而且$p^2+q^2=5$.

13. 求正整数p,q,使得 $2pq=12,p^2-q^2=5$ 而且 $p^2+q^2=13$.

14. 求正整数 p,q,使得 $p^2-q^2=7,p^2+q^2=25$,并利用这些p,

表 5.1

0									
1	2								
4	5	8							
9	10	13	18						
16	17	20	25	32					
25	26	29	34	41	50				
36	37	40	45	52	61	72			
49	50	53	58	65	74	85	98		
64	65	68	73	80	89	100	113	128	
81	82	85	90	97	106	117	130	145	162
100	101	104	109	116	125	136	149	164	181
121	122	125	130	137	146	157	170	185	202
144	145	148	153	160	169	180	193	208	225
169	170	173	178	185	194	205	218	233	250
196	197	200	205	212	221	232	245	260	277
225	226	229	234	241	250	261	274	289	306
256	257	260	265	272	281	292	305	320	337
289	290	293	298	305	314	325	338	353	370
324	325	328	333	340	349	360	373	388	405
361	362	365	370	377	386	397	410	425	442
400	401	404	409	416	425	436	449	464	481
441	442	445	450	457	466	477	490	505	522
484	485	488	493	500	509	520	533	548	565
529	530	533	538	545	554	565	578	593	610
576	577	580	585	592	601	612	625	640	657
625	626	629	634	641	650	661	674	689	706
676	677	680	685	692	701	712	725	740	757
729	730	733	738	745	754	765	778	793	810
784	785	788	793	800	809	820	833	848	865
841	842	845	850	857	866	877	890	905	922
900	901	904	909	916	925	936	949	964	981
961	962	965	970	977	986	997	1010	1025	1042
1024	1025	1028	1033	1040	1049	1060	1073	1088	1105
1089	1090	1093	1098	1105	1114	1125	1138	1153	1170
1156	1157	1160	1165	1172	1181	1192	1205	1220	1237
1225	1226	1229	1234	1241	1250	1261	1274	1289	1306
1296	1297	1300	1305	1312	1321	1332	1345	1360	1377
1369	1370	1373	1378	1385	1394	1405	1418	1433	1450
1444	1445	1448	1453	1460	1469	1480	1493	1508	1525
1521	1522	1525	1530	1537	1546	1557	1570	1585	1602
1600	1601	1604	1609	1616	1625	1636	1649	1664	1681
1681	1682	1685	1690	1697	1706	1717	1730	1745	1762
1764	1765	1768	1773	1780	1789	1800	1813	1828	1845
1849	1850	1853	1858	1865	1874	1885	1898	1913	1930
1936	1937	1940	1945	1952	1961	1972	1985	2000	2017
2025	2026	2029	2034	2041	2050	2061	2074	2089	2106
2116	2117	2120	2125	2132	2141	2152	2165	2180	2197
2209	2210	2213	2218	2225	2234	2245	2258	2273	2290
2304	2305	2308	2313	2320	2329	2340	2353	2368	2385
2401	2402	2405	2410	2417	2426	2437	2450	2465	2482
2500	2501	2504	2509	2516	2525	2536	2549	2564	2581

200										
221	242									
244	265	288								
269	290	313	338							
296	317	340	365	392						
325	346	369	394	421	450					
356	377	400	425	452	481	512				
389	410	433	458	485	514	545	578			
424	445	468	493	520	549	580	613	648		
461	482	505	530	557	586	617	650	685	722	
500	521	544	569	596	625	656	689	724	761	800
541	562	585	610	637	666	697	730	765	802	841
584	605	628	653	680	709	740	773	808	845	884
629	650	673	698	725	754	785	818	853	890	929
676	697	720	745	772	801	832	865	900	937	976
725	746	769	794	821	850	881	914	949	986	1025
776	797	820	845	872	901	932	965	1000	1037	1076
829	850	873	898	925	954	985	1018	1053	1090	1129
884	905	928	953	980	1009	1040	1073	1108	1145	1184
941	962	985	1010	1037	1066	1097	1130	1165	1202	1241
1000	1021	1044	1069	1096	1125	1156	1189	1224	1261	1300
1061	1082	1105	1130	1157	1186	1217	1250	1285	1322	1361
1124	1145	1168	1193	1220	1249	1280	1313	1348	1385	1424
1189	1210	1233	1258	1285	1314	1345	1378	1413	1450	1489
1256	1277	1300	1325	1352	1381	1412	1445	1480	1517	1556
1325	1346	1369	1394	1421	1450	1481	1514	1549	1586	1625
1396	1417	1440	1465	1492	1521	1552	1585	1620	1657	1696
1469	1490	1513	1538	1565	1594	1625	1658	1693	1730	1769
1544	1565	1588	1613	1640	1669	1700	1733	1768	1805	1844
1621	1642	1665	1690	1717	1746	1777	1810	1845	1882	1921
1700	1721	1744	1769	1796	1825	1856	1889	1924	1961	2000
1781	1802	1825	1850	1877	1906	1937	1970	2005	2042	2081
1864	1885	1908	1933	1960	1989	2020	2053	2088	2125	2164
1949	1970	1993	2018	2045	2074	2105	2138	2173	2210	2249
2036	2057	2080	2105	2132	2161	2192	2225	2260	2297	2336
2125	2146	2169	2194	2221	2250	2281	2314	2349	2386	2425
2216	2237	2260	2285	2312	2341	2372	2405	2440	2477	2516
2309	2330	2353	2378	2405	2434	2465	2498	2533	2570	2609
2404	2425	2448	2473	2500	2529	2560	2593	2628	2665	2704
2501	2522	2545	2570	2597	2626	2657	2690	2725	2762	2801
2600	2621	2644	2669	2696	2725	2756	2789	2824	2861	2900

q 构造一个 Pythagoras 三元数组.

15. 设 (x,y,z) 是本原 Pythagoras 三元数组且 x 是偶数,证明

(i) $z+y$ 是偶数,

(ii) $z-y$ 是偶数,

(iii) $\gcd(z+y,z-y)=2$,

(iv) $\frac{1}{2}(z+y)$ 与 $\frac{1}{2}(z-y)$ 是平方数.

令 $p^2=\frac{1}{2}(z+y), q^2=\frac{1}{2}(z-y)$, 证明 $x=2pq, y=p^2-q^2$, $z=p^2+q^2$, 而且 p 与 q 没有公因数.

16. 设 $(2pq, p^2-q^2, p^2+q^2)$ 是本原 Pythagoras 三元数组, 那么 p 与 q 能否都是偶数? 能否都是奇数?

17. 设 (x, y, z) 是本原 Pythagoras 三元数组, 证明 $(2xy, \pm(x^2-y^2), x^2+y^2)$ 也是本原 Pythagoras 三元数组; 此外, 若 x 是偶数, 则 $(2xz, z^2-x^2, z^2+x^2)$ 是另一个本原 Pythagoras 三元数组.

证明存在非零整数 a, b, c, 使得 $a^2+b^2=c^4$, 以及还存在非零整数 a,b,c, 使得 $a^2+b^4=c^2$.

18. 不同的本原 Pythagoras 三元数组的个数是否无限?

方程 $x^4+y^4=z^4$

19.

1						
16	17					
81	82	97				
256	257	272	337			
625	626	641	706	881		
1296	1297	1312	1377	1552	1921	
2401	2402	2417	2482	2657	3026	3697

上表中, 第一列是四次幂, 其它的列则是由第一列分别加上 1^4, $2^4, \cdots, 6^4$ 后得到.

除第一列外，表内有没有平方数？

20. 将问题 19 中的表向下延伸，如果在第一列之外有平方数，那么就存在整数 x, y, z，使得 $x^4+y^4=z^2$.

设 z^2 是表中不在第一列上的最小的平方数，那么 (x^2, y^2, z) 是本原 Pythagoras 三元数组；再设 x^2 是偶数，那么根据问题 15，就存在正整数 p, q, $\gcd(p, q)=1$,使得 $x^2=2pq$, $y^2=p^2-q^2$, $z=p^2+q^2$. 利用问题 16 证明 (q, y, p)是本原 Pythagoras 三元数组，而且 q 是偶数，p 是奇数. 再根据问题 15，存在整数 a, b, $\gcd(a, b)=1$，使得 $q=2ab$, $y=a^2-b^2$ 及$p=a^2+b^2$. 三个数 a, b, a^2+b^2 中的任意两个数能否有公因数？将 x^2 用 a, b 表示并且证明 a, b 和 a^2+b^2 都是平方数. 证明在这个四次方和的表中，p 是小于 z^2 的平方数.

21. 上题中推出的矛盾证明了不存在满足 $x^4+y^4=z^2$的非零整数 x, y, z. 证明不存在非零整数 x, y, z，使得 $x^4+y^4=z^4$. 事实上，对于任何整数 m，不存在非零整数 x，y，z，使得 $x^{4m}+y^{4m}=z^{4m}$.

22. 如果存在正整数 x, y, z 使得

$$x^4+y^2=z^4,$$

那么我们考虑具有最小 z 的本原 Pythagoras 三元数组 (x^2, y, z^2). 如果 y 是偶数，由等式 $y=2pq$，$x^2=p^2-q^2$，$z^2=p^2+q^2$ 得到 $q^4+(xz)^2=p^4$，这与 z 的最小性矛盾.

23. 设 (x^2, y, z^2)是本原 Pythagoras 三元数组而且 y 是奇数，利用等式 $x^2=2pq$, $y=p^2-q^2$, $z^2=p^2+q^2$ 证明存在互素的正整数 a, b，使得$\{p, q\}=\{2ab, a^2-b^2\}$. 三个数 a，b，a^2-b^2 中的任意两个数能否有公因数？将 x^2 用 a, b 表示，并且证明这三个数都是平方数. 比较等式

$$b^2+\left(\frac{x^2}{4ab}\right)=a^2$$

与 $x^4+y^2=z^4$，又得到和问题 22 中 z 的最小性相矛盾的结果.

方程 $x^2+y^2+z^2=t^2$

24. 通过考察对模 4 的各种可能性，确定是否存在整数 x,y,z,t 满足 $x^2+y^2+z^2=t^2$，并且使得

(i) x,y,z 都是奇数，

(ii) x,y 是奇数但 z 是偶数.

25. 设 x,y,z,t 是使 $x^2+y^2+z^2=t^2$ 的整数，证明它们之中至少有一个被 3 整除.

26. 设 x,y,z,t 是使 $x^2+y^2+z^2=t^2$ 成立的整数而且 x,y 是偶数，证明 z 与 t 有相同的奇偶性，因而 $t+z$ 与 $t-z$ 都是偶数. 令 $l=\frac{1}{2}x$，$m=\frac{1}{2}y$，$n=\frac{1}{2}(t-z)$，证明 $n\mid l^2+m^2$. 将 z 用 l,m,n 表示，证明 $l^2+m^2>n^2$.

正整数组 $\{z,t\}$ 的哪两组值，使得 $26^2+8^2+z^2=t^2$？

方程 $x^3+y^3=z^3$

问题 27__68 要证明，使得 $x^3+y^3=z^3$ 的非零整数 x,y,z 是不存在的. 本书的以后章节与这一节无关.

27. 表 5.2 列出了立方和（删去了重复部分）. 除了第一列外，表中有无另外的立方数？利用第一列及 $11^3=1331$，$12^3=1728$.

28. 如果存在整数 x,y,z，使得 $x^3+y^3=z^3$，那么它们之中可能有几个偶数？

表 5.2

−1000	−999	−992	−973	−936	−875	−784	−657	−488	−271	
−729	−728	−721	−702	−665	−604	−513	−385	−217		
−512	−511	−504	−485	−448	−387	−296	−169			
−343	−342	−335	−316	−279	−218	−127				
−216	−215	−208	−189	−152	−91					
−125	−124	−117	−98	−61						
−64	−63	−56	−37							
−27	−26	−19								
−8	−7									
−1										
1	2									
8	9	16								
27	28	35	54							
64	65	72	91	128						
125	126	133	152	189	250					
216	217	224	243	280	341	432				
343	344	351	370	407	468	559	686			
512	513	520	539	576	637	728	855	1024		
729	730	737	756	793	854	945	1072	1241	1458	
1000	1001	1008	1027	1064	1125	1216	1343	1512	1729	2000

29. 如果存在整数 x，y，z，使得 $x^3+y^3=z^3$，那么它们之中可能有几个被 7 整除？

利用表 3.2 做一个 Z_7 中的立方和表.

30. 如果存在整数 x，y，z，使得 $x^3+y^3=z^3$，那么它们之中可能有几个被 13 整除？

利用表 3.2 做一个 Z_{13} 中的立方和表.

31. 如果存在整数x，y，z，使得 $x^3+y^3=z^3$，说明为什么有 $x+y\equiv z \pmod 3$，并且证明 $(x+y-z)^3$ 有因数27．展开乘积 $(x+y-z)^3$ 并且证明 $(x+y)(x-z)(y-z)$有因数9．

证明 x，y，z 中有一个被 3 整除．

32. 如果 $x^3+y^3=z^3$ 有非零整数解 x，y，z，那么它是否必有满足 $\gcd(x,y,z)=1$ 的解？

33. 在圆心坐标为 $(0,0)$、半径为 1 的圆上画一个内接正六边形．若它的一个顶点是 $(1,0)$，求另外五个顶点的坐标．

34. 上题中，把 x 坐标为负、y 坐标为正的顶点记为 ω．设 $\omega=(a,b)$①，求出复数 $(a+ib)^2=\omega^2$ 及 $(a+ib)^3=\omega^3$．

证明六边形的顶点可以在 Argand 图上相应地用 ± 1，$\pm\omega$，$\pm\omega^2$ 标出．

用复数表示这些点时，它们是否构成一个乘法群？求 $1+\omega+\omega^2$．

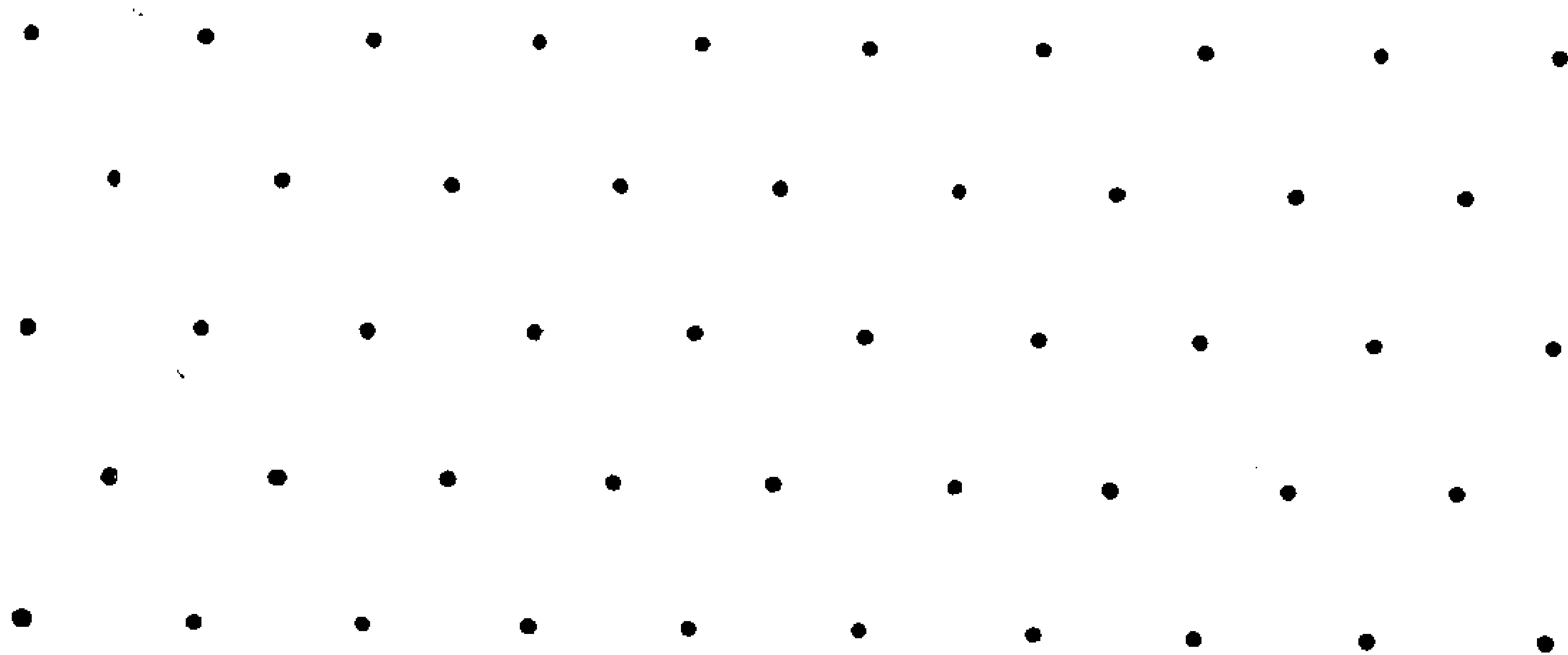


图 5.2

一个等距格是由全等的等边三角形组成的规则的棋盘式结构．在本章的余下部分，所谓格点是指等距格中格线的交点（见

① 按通常的意义，ω 又表示复数 $a+bi$．——译者注．

图 5.2)，或者等价地，是指这个棋盘式结构中的等边三角形的顶点．我们要来说明将整数对与这种格点相对应的可能性．

35. 在等距格上，先选定两个靠得最近的格点，把它们标为 0 和 1，再把所有的格点看做一个 Argand 图上的点．然后，按问题 34 的约定，把相应的点标上 ω．标出与 ± 1，± 2，± 3，± 4 以及 $\pm\omega$，$\pm 2\omega$，$\pm 3\omega$，$\pm 4\omega$ 相对应的格点．按照通常对复数 (看成是 Argand 图上的点时)的加法和平面矢量加法的规定，$\alpha+\beta$ 到点 0 的距离二倍于点 0 到连结 α 与 β 的线段中点的距离，点 0，α，β，$\alpha+\beta$ 构成平行四边形，由此确定等距格上的所有格点是否都可以用 $a+b\omega$ 形式的元素来标出，其中 a，b 是整数．

36. 求整数 a，b，c，d，使得 $\omega^2=a+b\omega$ 而且 $-\omega^2=c+d\omega$．

37. 作为复数的子集，集合 $Z[\omega]=\{a+b\omega \mid a, b\in Z\}$ 是否构成一个加法群？ 集合 $Z[\omega]$ 对于乘法是不是封闭的？ $Z[\omega]$ 的非零元素是否构成乘法群？

38. 化简以下乘积：

$$(1+\omega)(1+\omega^2),\ (a+b\omega)(a+b\omega^2),$$
$$(1-\omega)(1-\omega^2),\ (a-b\omega)(a-b\omega^2).$$

39. 设 a，b 是整数，在 $Z[\omega]$ 中将

$$3,\ a^2-ab+b^2,\ a^2+ab+b^2,\ a^3+b^3,\ a^3-b^3$$

分解因式．

40. 因为 $a+b\omega=(a-\frac{1}{2}b)+i\frac{1}{2}b\sqrt{3}$，所以模[①]

$$|a+b\omega|=\sqrt{(a-\frac{1}{2}b)^2+\frac{3}{4}b^2}.$$

证明 $|a+b\omega|^2$ 是整数，而且除 $a+b\omega=0$ 外，它总是正的．

41. 称 $N(a+b\omega)=a^2-ab+b^2$ 为 $a+b\omega$ 的范数，其中

---

① 这是指复数的模．——译者注．

$a,b\in \mathbf{Z}$.对于 $\alpha,\beta\in \mathbf{Z}[\omega]$，验证等式

$$N(\alpha\beta)=N(\alpha)N(\beta).$$

42. 参照问题 35，列出 $\mathbf{Z}[\omega]$ 中使得

(i) $N(\alpha)=0$， (ii) $N(\alpha)=1$， (iii) $N(\alpha)=2$，

(iv) $N(\alpha)=3$， (v) $N(\alpha)=4$

的元素 α.

43. 设 $\alpha,\beta\in \mathbf{Z}[\omega]$ 且 $\alpha\beta=1$，证明 $N(\alpha)N(\beta)=1$，并找出 $\mathbf{Z}[\omega]$ 中乘法逆元素仍属于该集合的所有元素．这六个元素称为 $\mathbf{Z}[\omega]$ 的**单位元素**[①].

44. 求出十个三元数组 $[\alpha,\beta,\gamma]$ (不计顺序)，使得 $\alpha,\beta,\gamma\in \mathbf{Z}[\omega]$ 而且 $\alpha\beta\gamma=1$.

45. 令 $\lambda=1+2\omega$．按问题 35 的规定，在等距格上标出点 $\pm\lambda$，$\pm 2\lambda$，$\pm\omega\lambda$，$\pm\omega^2\lambda$，$\pm\lambda^2$，$\pm\omega\lambda^2$，$\pm\omega^2\lambda^2$，$\pm\lambda\pm 1$，$\pm 2\lambda\pm 1$，$\pm\omega\lambda\pm 1$，$\pm\omega^2\lambda\pm 1$．能否画出一组平行线只通过对应 λ 倍数[②]的格点？

46. 证明不存在 $\alpha\in \mathbf{Z}[\omega]$，使得 $\alpha\lambda=1$，因此 1 不是 λ 的倍数．在格上标出与 (λ 的倍数) $+1$ 对应的格点．你能画出一组仅含这种格点的平行线吗？ 证明不存在 $\alpha,\beta\in \mathbf{Z}[\omega]$，使得 $\alpha\lambda=\beta\lambda+1$.

47. 证明在 $\mathbf{Z}[\omega]$ 中 -1 不是 λ 的倍数．

标出与 (λ 的倍数) -1 对应的格点．

证明不存在 $\alpha,\beta\in \mathbf{Z}[\omega]$，使得 $\alpha\lambda=\beta\lambda-1$.

48. 证明在 $\mathbf{Z}[\omega]$ 中 2 不是 λ 的倍数．证明不存在 $\alpha,\beta\in \mathbf{Z}[\omega]$，使得 $\alpha\lambda+1=\beta\lambda-1$.

49. 设 a,b 是整数，证明 $a+b\omega=a+b+$ (λ 的倍数).

利用 $\lambda^2=-3$ 这个事实证明：若 $\alpha\in \mathbf{Z}[\omega]$，则 $\alpha\equiv 0,1$ 或 $-1 \pmod{\lambda}$[③].

---

① 或称单位元.

② 设 $\mu,\gamma\in \mathbf{Z}[\omega]$，如果存在 $\nu\in \mathbf{Z}[\omega]$ 使得 $\mu=\gamma\nu$，则称在 $\mathbf{Z}[\omega]$ 中，μ 是 γ 的倍数.

③ 设 $\alpha,\beta,\gamma\in \mathbf{Z}[\omega]$，如果 $\alpha-\beta$ 是 γ 的倍数，则记做 $\alpha\equiv\beta \pmod{\gamma}$.—— 以上均为译者注.

50. 在 $Z[\omega]$ 中，使 $\alpha\beta=\lambda$ 成立的数对 $\{\alpha,\beta\}$ 会是哪六个？

51. 若 $\gamma\in Z[\omega]$ 不是单位元，而且 γ 的因子只是单位元，或者是 γ 与单位元的乘积，则称 γ 是 $Z[\omega]$ 中的素元. 2，3 及 λ 是不是 $Z[\omega]$ 中的素元？

52. 求有理数 u，v，使得

$$\frac{6+7\omega}{2+3\omega}=u+v\omega,$$

此处是复数的除法. (如果你愿意的话，可以利用问题 38). 选取离 u 最近的整数 U，以及离 v 最近的整数 V，并令 $u=U+u'$，$v=V+v'$，验证 $(2+3\omega)(u'+v'\omega)$ 是 $Z[\omega]$ 中的元素，而且 $N[(2+3\omega)(u'+v'\omega)]<N(2+3\omega)$.

53. 设 $\alpha=a+b\omega\in Z[\omega]$，$\beta=c+d\omega\in Z[\omega]$ 而且 $\beta\neq 0$，证明 $\frac{\alpha}{\beta}=u+v\omega$，其中 u，v 是两个有理数. 选取离 u 最近的整数 U，以及离 v 最近的整数 V，令 $u=U+u'$，$v=V+v'$，说明 $|u'|$，$|v'|\leqslant\frac{1}{2}$ 的原因，并推出 $|u'^2-u'v'+v'^2|\leqslant\frac{3}{4}$.

证明 $(c+d\omega)(u'+v'\omega)\in Z[\omega]$ 与 $N[(c+d\omega)(u'+v'\omega)]<N(c+d\omega)$.

记 $q=U+V\omega$，证明 $\alpha=\beta q+r$ 且 $N(r)<N(\beta)$.

54. 给定 $Z[\omega]$ 中的元素 α 与 β，集合 $A=\{x\alpha+y\beta\mid x,y\in Z[\omega]\}$ 是不是 $(Z[\omega],+)$ 的子群？ 与问题 1.29 的论证做个比较. 设 $\delta\in A$ 是 A 中有最小非零范数的元素，利用类似于问题 1.33 与问题 1.34 的论证，证明

(i) 存在 x_1，y_1，使得 $\delta=x_1\alpha+y_1\beta$，

(ii) α 与 β 的每个公因子都是 δ 的因子，

(iii) α 与 β 都是 δ 的倍数 (利用问题 53)，

(iv) A 由 δ 的所有倍数组成.

我们记 $\delta=\gcd(\alpha,\beta)$.

55. 设 π，α，$\beta\in Z[\omega]$，π 是素元而且 $\pi\mid\alpha\beta$，但是 π 不整除 α，那么 $(Z[\omega],+)$ 的子群 $A=\{x\pi+y\alpha\mid x,y\in Z[\omega]\}$ 是什么？

证明存在 x, y，使得 $x\pi + y\alpha = 1$.

把问题 1.52 的论证做些变化，证明 $\pi \mid \beta$.

56. 设 $\pi_1, \pi_2, \cdots, \pi_n$ 及 $\gamma_1, \gamma_2, \cdots, \gamma_m$ 都是 $\mathrm{Z}[\omega]$ 中的素元而且

$$\pi_1\pi_2\cdots\pi_n = \gamma_1\gamma_2\cdots\gamma_m,$$

证明 π_1 等于这些 γ_i 中的某一个乘以单位元．两边除以 π_1 后，证明 π_2 等于这些 γ_i 中的另一个乘以单位元．对因子个数施行归纳法，证明 $n=m$ 而且这些 π_i 中的每一个等于这些 γ_i 中的一个乘以单位元．

($\mathrm{Z}[\omega]$ 中的因子分解唯一性定理)．

57. 若有非零整数 x, y, z 满足 $x^3+y^3=z^3$，那么这个方程在 $\mathrm{Z}[\omega]$ 中是否有解？

58. 若有非零的 $x, y, z \in \mathrm{Z}[\omega]$ 使得 $x^3+y^3=z^3$，那么是否有非零的 $\alpha, \beta, \gamma \in \mathrm{Z}[\omega]$，使得 $\alpha^3+\beta^3+\gamma^3=0$？

59. 若有非零的 $x, y, z \in \mathrm{Z}[\omega]$，使得 $x^3+y^3+z^3=0$，那么是否存在非零的 $\alpha, \beta, \gamma \in \mathrm{Z}[\omega]$，使得 $\alpha^3+\beta^3+\gamma^3=0$，而且它们之中的任何两个数都没有公共素因子？

60. 设 $x=\alpha\lambda+1$，其中 λ 见于问题 45，证明 $x^3-1=\alpha(\alpha^2-1)\lambda^3-\alpha^2\lambda^4$.

说明为什么 α，或 $\alpha-1$，或 $\alpha+1$ 有因子 λ，并证明 $x^3 \equiv 1 \pmod{\lambda^4}$.

设 $x=\alpha\lambda-1$，证明 $x^3 \equiv -1 \pmod{\lambda^4}$.

61. 设 $x^3+y^3+z^3 \equiv 0 \pmod 9$，证明假设“$x, y, z$ 都没有因子 λ”是错误的．

62. 设 $x^3+y^3+z^3=0$，而且 λ 是 x 的因子但不是 y 和 z 的因子，求 $y^3+z^3 \pmod{\lambda}$ 所可能取的值，并且判断 y 与 z 能否对模 λ 同余．

63. 设 $y=\alpha\lambda+1$ 且 $z=\beta\lambda-1$，证明 $y+\omega z$，$\omega y+z$ 以及 $y+z$ 都含有因子 λ．此外，如果 $\delta\lambda$ 是这些数当中任何两个数的

公因子，那么δ是单位元，或是y与z的公因子．因此，这些数当中至多有一个数含有因子λ^2．

64. 设$x^3+y^3+z^3=0$，$\lambda|x$，但λ不是y或z的因子，证明$x^3\equiv 0 \pmod{\lambda^4}$并推出$\lambda^2|x$．

65. 设$x^3+y^3+z^3=0$，证明

$$-x^3=\omega^2(y+z)(\omega y+z)(y+\omega z).$$

若x，y，z没有公共素因子且$\lambda|x$，利用问题62与问题63，证明

$$\frac{\omega^2(y+z)}{\lambda},\quad \frac{\omega y+z}{\lambda} \text{ 与 } \frac{y+\omega z}{\lambda}$$

都是$Z[\omega]$中的一个立方数与一个单位元之积．此外，它们之中任何一个所含λ的最高幂次数都小于x^3所含λ的最高幂次数，但是不小于1（根据问题64）．

66. (i) 通过考察范数，证明$Z[\omega]$中不存在元素π，使得

$\pi\lambda^3=1+\omega$，$1-\omega$，$-1+\omega$或$-1-\omega$．

(ii) 设α，β和γ是$Z[\omega]$中的非零元素而且λ只整除α，β或γ中的一个，证明等式

$$\alpha^3+\omega\beta^3+\omega^2\gamma^3=0$$

不可能成立．

67. 对于任意的y和z，证明

$$\frac{\omega^2(y+z)}{\lambda}+\frac{\omega y+z}{\lambda}+\frac{y+\omega z}{\lambda}=0.$$

利用问题65，问题44和问题66，证明：若$x^3+y^3+z^3=0$而且$\lambda|x$，但是λ不整除y和z，则可构造一个等式$\alpha^3+\beta^3+\gamma^3=0$，其中$\lambda|\alpha$但$\lambda$不整除$\beta$与$\gamma$，而且能够整除$\alpha$的$\lambda$的最高幂次数小于能整除$x$的$\lambda$的最高幂次数．重复这一过程就得到与问题61矛盾的结果，从而证明不存在满足$x^3+y^3+z^3=0$的非零整数x，y，z．

68. 证明：对于任何非零整数m，不存在非零整数x，y，z，使得

$x^{3m}+y^{3m}=z^{3m}$.

注记与答案

参考书见书目：Sierpinski (1962), Bolker (1970).

1. 25, 100, 169, 225, 289, 400, 625 (二次), 676, 841, 900, 1156, 1369, 1521, 1681, 2500, 2704.

2. 25, 100, 225, 400, 625, 900.

$4^2+3^2=5^2 \Rightarrow (4n)^2+(3n)^2=(5n)^2$.

3. 169, 676, 1521, 2704.

$12^2+5^2=13^2 \Rightarrow (12n)^2+(5n)^2=(13n)^2$.

4. $48^2+14^2=50^2=2500$, $30^2+16^2=34^2=1156$.

5. (4, 3, 5), (12, 5, 13), (24, 7, 25), (15, 8, 17), (35, 12, 37), (21, 20, 29), (40, 9, 41).

边长为整数的直角三角形称为 Pythagoras 三角形．每一个 Pythagoras 三元数组对应着一个 Pythagoras 三角形，反之亦然．由表 5.1 得到的 Pythagoras 三角形可用图 5.3 解释．每个画圈的格点是一个 Pythagoras 三角形的顶点，这个三角形还有一个顶点在 O，它有两条边与格线平行．在过 O 点的每条直线上，至多有一个画圈的格点和一个本原 Pythagoras 三元数组对应．

6. (i) $8^2+6^2=10^2$．(ii)由两个是偶数推出三个都是偶数．(iii) $4^2+3^2=5^2$．(iv)若 x, y 是奇数，则 x^2, y^2 是奇数，所以 z^2 是偶数，z 也是偶数．参看问题 9．

7. (i) $12^2+9^2=15^2$．(ii)由两个被 3 整除推出全都被 3 整除．(iii) $4^2+3^2=5^2$．(iv)因为 $z^2 \not\equiv 2 \pmod 3$，所以 x 或 $y \equiv 0 \pmod 3$．

x^2+y^2	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

8. (i) $20^2+15^2=25^2$.

(ii)两个被 5 整除推出全都被 5 整除.

(iii) $4^2+3^2=5^2$.

(iv)因为 $z^2 \not\equiv 2, 3 \pmod 5$，所以 x，或 y，或 $z \equiv 0 \pmod 5$.

x^2+y^2	0	1	2	3	4
0	0	1	4	4	1
1	1	2	0	0	2
2	4	0	3	3	0
3	4	0	3	3	0
4	1	2	0	0	2

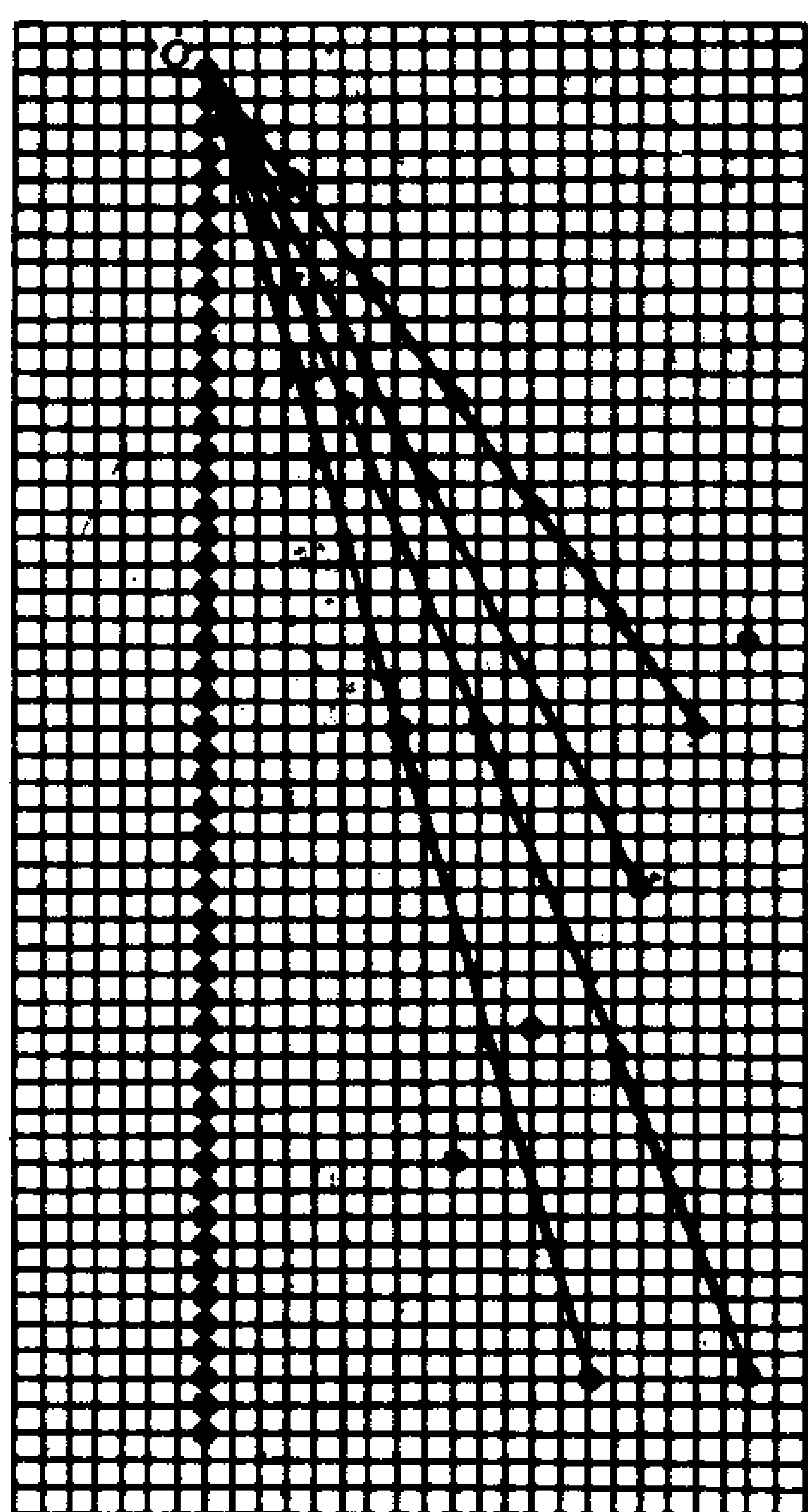


图 5.3

9. x^2+y^2

	0	1	2	3
0	0	1	0	1
1	1	2	1	2
2	0	1	0	1
3	1	2	1	2

因为 $z^2 \not\equiv 2 \pmod 4$，所以由 z^2 是偶数推出 $z^2 \equiv 0 \pmod 4$，这又推出 $x^2 \equiv y^2 \equiv 0 \pmod 4$.

令 $y=2k+1$，$z=2h+1$，则

$$x^2=z^2-y^2$$
$$=4h^2+4h-(4k^2+4k)$$
$$=4h(h+1)-4k(k+1).$$

$h(h+1)$与 $k(k+1)$都是偶数，所以 $8|x^2$，$4|x$．由问题6，问题 7，问题8 及问题 9 可以推出，构成 Pythagoras 三元数组的三个数中，能被3 整除，被 4 整除，被5 整除的数，都至少有一 个.

10. 已知 $x^2+y^2=z^2$，于是

$2x(y+z):((y+z)^2-x^2):((y+z)^2+x^2)$
$=2x(y+z):2y(y+z):2z(y+z)$.

12. $p=2$，$q=1$.

13. $p=3$，$q=2$.

14. $p=4$，$q=3$ ，$(24, 7, 25)$.

15. 根据问题 6，y 和 z 是奇数，所以 $z+y$ 与 $z-y$ 是偶数.

若 $\gcd(z+y, z-y)=2d$，则 $2d\mid(z+y)+(z-y)$，所以 $d\mid z$；又有 $2d\mid(z+y)-(z-y)$，所以 $d\mid y$. 但是 $\gcd(y, z)=1$，所以 $d=1$.

$\left[\frac{1}{2}(z-y)\right]\left[\frac{1}{2}(z+y)\right]=\left(\frac{1}{2}x\right)^2$. 但是 $\gcd\left(\frac{1}{2}(z+y), \frac{1}{2}(z-y)\right)=1$，所以这两个数都是平方数. 若 $d\mid p, q$，则 $d^2\mid x, y, z$，所以 $d=1$.

16. 若 p 和 q 有相同的奇偶性，那么这个三元数组中的三个数都是偶数，所以它不是本原的.

17. 根据问题 6 和问题 9，x 与 y 的奇偶性是不同的，所以 x^2-y^2 与 x^2+y^2 都是奇数. 若 $d\mid x^2-y^2, x^2+y^2$，则 d 是奇数，但是 $d\mid 2x^2, 2y^2$，所以 $d\mid x, y$，因此 $d=1$. 类似地，x 与 z 的奇偶性不同，可做同样的讨论.

18. 在问题 17 中，第二次构造的三元数组中的 z 是变大了，所以这样构造出的三元数组永远不会重复.

19. 没有.

20. 由问题 6 和问题 9 知道，x^2 或者 y^2 必有一个是偶数. 不失一般性，设 x^2 是偶数. 根据问题 16，p 和 q 没有公约数，因此 (q, y, p) 是本原的. 因为 y 是奇数，所以，由问题 6 和问题 9 知道 q 是偶数. 对任意的素数 d，若 $d\mid a, a^2+b^2$，则 $d\mid b^2$. 所以 $d\mid b$. 但是 $\gcd(a, b)=1$，所以 $d=1$. 同理，$\gcd(b, a^2+b^2)=1$. 由于 $x^2=2(a^2+b^2)2ab$，所以 $\left(\frac{1}{2}x\right)^2=ab(a^2+b^2)$. 因为

右端的三个因数互素，所以它们都是平方数．这样，a^2 与 b^2 是四次方数，a^2+b^2 是平方数且 $p=a^2+b^2$．因为 $\gcd(a,b)=1$，所以此处的 Pythagoras 三元数组是本原的．但是，由于 $p<p^2<p^2+q^2=z<z^2$，这和 z 的最小性矛盾．

倘使我们不要求 z 是最小的这种数，那么就可以找到一个更小的 z．这样，由 Fermat 的"递降法"就会推出一个矛盾，因为在正整数中的一个反复递减方法必定是有终结的．"递降法"等价于"良序原则"，即每个非空的正整数集合中有最小数，而这又等价于数学归纳原理．

21．形如 (x^2, y^2, z^2) 的 Pythagoras 三元数组必具有 (x^2, y^2, t) 的形式，所以不存在．

同样地，对于正数 m，形如 (x^{2m}, y^{2m}, z^{2m}) 的 Pythagoras 三元数组是不存在的．若 m 是负数，设 $m=-n$，则

$$x^{4m}+y^{4m}=z^{4m}\Longleftrightarrow(yz)^{4n}+(zx)^{4n}=(xy)^{4n},$$

后者同样是不可能的．

22．因为 $\gcd(p,q)=1$，所以 (q^2, xy, p^2) 是本原的，而且 $p^2<p^2+q^2=z^2$．

23．对于素数 d，若 $d|a$，a^2-b^2，则 $d|b^2$，$d|b$，但 $\gcd(a,b)=1$．$x^2=2\cdot 2ab\cdot(a^2-b^2)$，所以 $\left(\frac{1}{2}x\right)^2=ab(a^2-b^2)$，但是右端的三个因子互素，所以它们中的每一个都是平方数．现在，$b^2+\dfrac{x^2}{4ab}=a^2$ 是一个形如 $x^4+y^2=z^4$ 的等式，而且 $\gcd(a,b)=1$，所以此处的 Pythagoras 三元数组是本原的，而且 $a<2ab<p^2+q^2=z^2$．

24．若 x, y 是奇数，$x^2\equiv y^2\equiv 1 \pmod 4$，那么 $x^2+y^2\equiv 2 \pmod 4$．当 z 是偶数时，$x^2+y^2+z^2\equiv 2 \pmod 4$，当 z 是奇数时，$x^2+y^2+z^2\equiv 3 \pmod 4$．但是 $t^2\not\equiv 2, 3 \pmod 3$，所以 x, y, z 中至少有两个是偶数．

25．若 x, y, z 都不被 3 整除，那么 $x^2\equiv y^2\equiv z^2\equiv 1$

(mod 3)，所以 $x^2+y^2+z^2\equiv 0 \pmod 3$，因而 t 被 3 整除.

26. 若 x 与 y 是偶数，则由 $t^2-z^2=x^2+y^2$ 推出 $t^2\equiv z^2 \pmod 2$. 于是 $t\equiv z \pmod 2$，而且 $t-z$ 与 $t+z$ 都 $\equiv 0 \pmod 2$. 由 $4l^2+4m^2=(t-z)(t+z)$ 得出

$$l^2+m^2=n\left[\frac{1}{2}(t+z)\right] \quad 及\ n\,|\,l^2+m^2.\ 由于$$

$z=\dfrac{l^2+m^2}{n}-n>0$，所以 $l^2+m^2>n^2$. 若 $l=13$，$m=4$，则

$l^2+m^2=185=5\cdot 37$，于是 $n=1$，5；$z=184$，32；$t=186$，42.

27. 没有.

28. 三个或一个.

29. Z_7 中的立方数只有 0，1，6. 因此，如果两个立方数之和等于一个立方数，那么或者是三个数中只有一个数同余于 0 (mod 7)，或者是三个数都同余于 0 (mod 7).

0	1	6
1	2	0
6	0	5

30. Z_{13} 中的立方数只有 0，1，5，8，12. 因此，如果两个立方数的和等于一个立方数，那么这三个立方数中有一个同余于 0 (mod 13).

0	1	5	8	12
1	2	6	9	0
5	6	10	0	4
8	9	0	3	7
12	0	4	7	11

31. 因为 $x^3\equiv x \pmod 3$，所以 $x+y\equiv z \pmod 3$，$x+y-z$ 有因数 3，以及 $(x+y-z)^3$ 有因数 27.

$$(x+y-z)^3=(x^3+y^3-z^3)+3(x+y)(x-z)(y-z).$$

这样，27 整除上式右端，所以 $9\mid(x+y)(x-z)(y-z)$，因此 $3\mid x+y$，或 $x-z$，或 $y-z$.

若 $3\mid x+y$，则由 $3\mid x+y-z$ 得出 $3\mid z$. 另外两种可能性导至 $3\mid y$ 或 $3\mid x$.

32. 若 $\gcd(x,y,z)=d$，则 $\left(\frac{x}{d}\right)^3+\left(\frac{y}{d}\right)^3=\left(\frac{z}{d}\right)^3$.

33. 顶点是 $(\pm 1,0)$，$\left(\pm\frac{1}{2},\pm\frac{1}{2}\sqrt{3}\right)$. 这里，我们开始来建立一个集合，在这个集合中比在 Z 中更容易对方程 $x^3+y^3=z^3$ 进行分析.

34. $\omega^2=-\frac{1}{2}-i\frac{\sqrt{3}}{2}$，$\omega^3=1$. 由 $-\omega$ 生成的 6 阶群.

36. $\omega^2=-1-\omega$，$-\omega^2=1+\omega$.

37. 是. 是. 2 在 $Z[\omega]$ 中没有乘法逆元素.

38. 1，a^2-ab+b^2，3，a^2+ab+b^2.

39. $3=(1-\omega)(1-\omega^2)$，$a^2-ab+b^2=(a+b\omega)(a+b\omega^2)$，$a^2+ab+b^2=(a-b\omega)(a-b\omega^2)$，$a^3+b^3=(a+b)(a+b\omega)\cdot(a+b\omega^2)$，$a^3-b^3=(a-b)(a-b\omega)(a-b\omega^2)$.

正是因为 x^3+y^3 在 $Z[\omega]$ 中有线性因子分解式，所以在这个集合中分析方程 $x^3+y^3=z^3$ 是合适的.

40. $$\left(a-\frac{1}{2}b\right)^2+\frac{3}{4}b^2=a^2-ab+\frac{1}{4}b^2+\frac{3}{4}b^2$$
$$=a^2-ab+b^2\in Z.$$

显然 $\left(a-\frac{1}{2}b\right)^2+\frac{3}{4}b^2\geqslant 0$，而且仅当 $b=0$，$a=0$ 时，它才取 0 值.

41. $N(\alpha)=|\alpha|^2$. 对于任意的复数 α，β，$|\alpha\beta|=|\alpha|\cdot|\beta|$. $N(\alpha\beta)=|\alpha\beta|^2=|\alpha|^2\cdot|\beta|^2=N(\alpha)N(\beta)$.

42. 画出以 O 为心、以 0，1，$\sqrt{2}$，$\sqrt{3}$，2 为半径的圆.

$N(\alpha)=0 \Rightarrow \alpha=0$. $N(\alpha)=1 \Rightarrow \alpha=\pm 1$, $\pm\omega$, $\pm\omega^2$. 不存在α，使得 $N(\alpha)=2$. $N(\alpha)=3 \Rightarrow \alpha=(1+2\omega)$乘以 ± 1，$\pm\omega$，$\pm\omega^2$. $N(\alpha)=4 \Rightarrow \alpha=2$ 乘以 ± 1，$\pm\omega$，$\pm\omega^2$.

43. 若 $\alpha\beta=1$，则 $N(\alpha\beta)=N(1)$，于是 $N(\alpha)N(\beta)=1$. 但 $N(\alpha)$与 $N(\beta)$是零或正整数，所以 $N(\alpha)=N(\beta)=1$. 这样，只有六个元素 ± 1，$\pm\omega$，$\pm\omega^2$ 能有乘法逆元素. Z 中的单位元是 ± 1.

44. $\alpha\beta\gamma=1 \Rightarrow N(\alpha)N(\beta)N(\gamma)=1$
$$\Rightarrow N(\alpha)=N(\beta)=N(\gamma)=1$$
$$\Rightarrow \alpha, \beta, \gamma=\pm 1, \pm\omega, \pm\omega^2.$$

$[\alpha, \beta, \gamma]=[1, 1, 1]$，$[1, -1, -1]$，$[\omega, \omega, \omega]$，
$[\omega^2, \omega^2, \omega^2]$，$[\omega, -\omega, -\omega]$，$[\omega^2, -\omega^2, -\omega^2]$，
$[1, \omega, \omega^2]$，$[1, -\omega, -\omega^2]$，$[-1, \omega, -\omega^2]$，
$[-1, -\omega, \omega^2]$.

45. 见图 5.4 .

46. $N(\alpha\lambda)=1 \Rightarrow N(\alpha)N(\lambda)=1$. 但 $N(\lambda)=3$，所以这样的 α 不存在. 若 $\alpha\lambda=\beta\lambda+1$，则 $(\alpha-\beta)\lambda=1$，但是这伴 的$\alpha-\beta$ 不存在.

47. $\alpha\lambda=-1 \Rightarrow N(\alpha)N(\lambda)=1$. 若 $\alpha\lambda=\beta\lambda-1$，则 $(\beta-\alpha)\lambda=1$，但这样的 $\beta-\lambda$ 是不存在的.

48. $\alpha\lambda=2 \Rightarrow N(\alpha)N(\lambda)=N(2) \Rightarrow N(\alpha)\cdot 3=4$，所以这样的 α 不存在. 若 $\alpha\lambda+1=\beta\lambda-1$，则$(\beta-\alpha)\lambda=2$，但这样的 $\beta-\alpha$ 不存在.

49. $(a+b\omega)-(a+b)=b(\omega-1)=\lambda b\omega^2$.

$a+b$ 是整数，所以它同余于 0，1 或 $-1 \pmod 3$.

50. $\{1, \lambda\}$，$\{-1, -\lambda\}$，$\{\omega, \omega^2\lambda\}$，$\{-\omega, -\omega^2\lambda\}$，$\{\omega^2, \omega\lambda\}$，$\{-\omega^2, -\omega\lambda\}$.

51. 若$\alpha\beta=2$，则 $N(\alpha)N(\beta)=4$. 但是没有α 能使$N(\alpha)=2$，所以 $N(\alpha)$或 $N(\beta)=1$，即 α 或 β 是单位元. 因此，2 是素元.

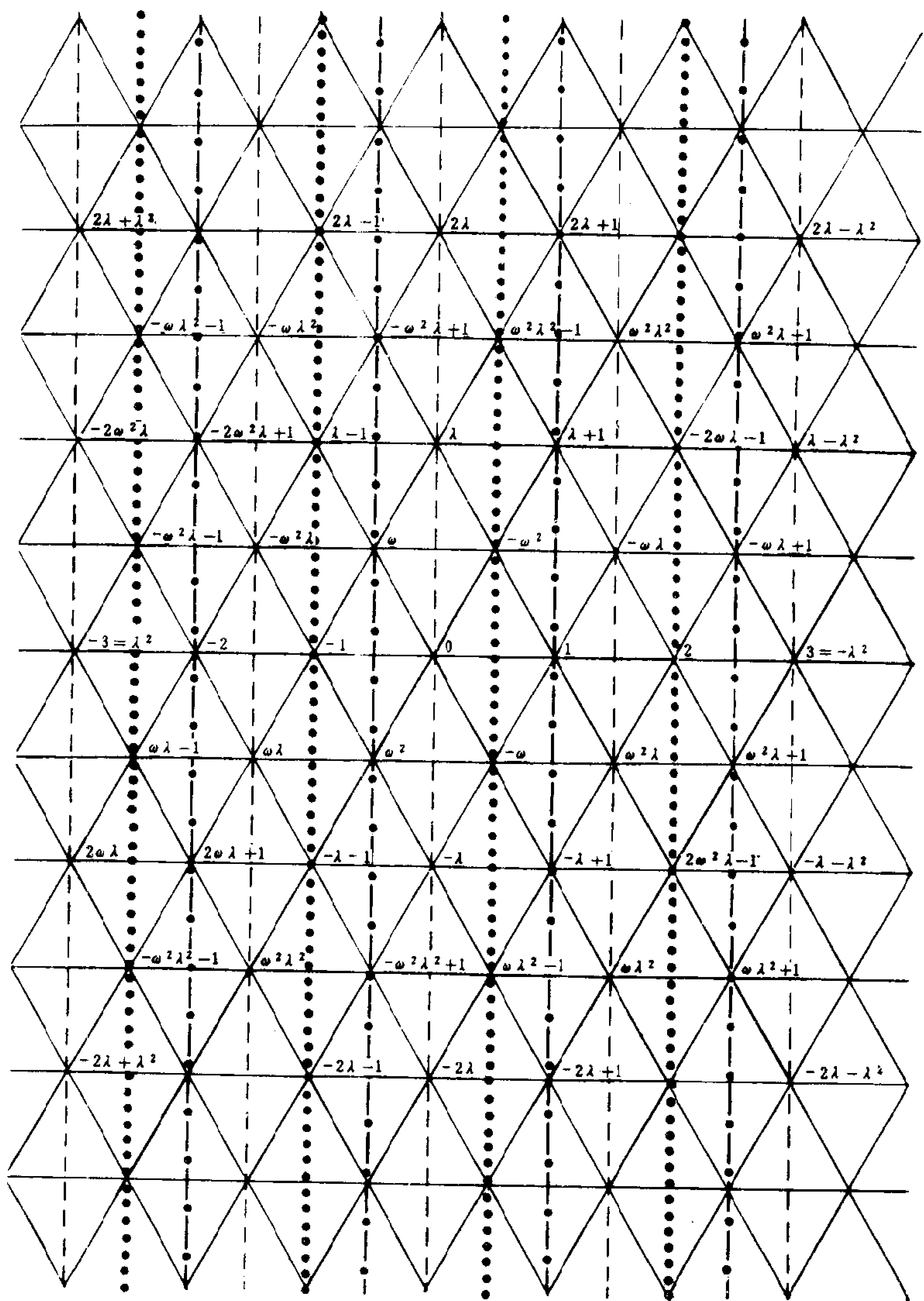

$2\lambda+\lambda^2$
$2\lambda-1$
2λ
$2\lambda+1$
$2\lambda-\lambda^2$
$-\omega\lambda^2-1$
$-\omega\lambda^2$
$-\omega^2\lambda+1$
$\omega^2\lambda^2-1$
$\omega^2\lambda^2$
$\omega^2\lambda+1$
$-2\omega^2\lambda$
$-2\omega^2\lambda+1$
$\lambda-1$
λ
$\lambda+1$
$-2\omega\lambda-1$
$\lambda-\lambda^2$
$-\omega^2\lambda-1$
$-\omega^2\lambda$
ω
$-\omega^2$
$-\omega\lambda$
$-\omega\lambda+1$
$-3=\lambda^2$
-2
-1
0
1
2
$3=-\lambda^2$
$\omega\lambda-1$
$\omega\lambda$
ω^2
$-\omega$
$\omega^2\lambda$
$\omega^2\lambda+1$
$2\omega\lambda$
$2\omega\lambda+1$
$-\lambda-1$
$-\lambda$
$-\lambda+1$
$2\omega^2\lambda-1$
$-\lambda-\lambda^2$
$-\omega^2\lambda^2-1$
$\omega^2\lambda^2$
$-\omega^2\lambda^2+1$
$\omega\lambda^2-1$
$\omega\lambda^2$
$\omega\lambda^2+1$
$-2\lambda+\lambda^2$
$-2\lambda-1$
-2λ
$-2\lambda+1$
$-2\lambda-\lambda^2$

图 5.4

$3=(-\lambda)\lambda$，所以3 不是素元．由问题 50 知道，λ 是素元．

52. $\dfrac{6+7\omega}{2+3\omega}=\dfrac{6+7\omega}{2+3\omega}\cdot\dfrac{2+3\omega^2}{2+3\omega^2}=\dfrac{33+14\omega+18\omega^2}{7}$

$$=\frac{15-4\omega}{7}.$$

$U=2$，$V=-1$；$(2+3\omega)\left(\dfrac{1}{7}+\dfrac{3}{7}\omega\right)=-1$；

$N(-1)<7=N(2+3\omega)$.

53. 将分子、分母同乘以 $c+d\omega^2$ 并化简．例如，若 $u=2\dfrac{1}{2}$，那么 U 可以有不同的选法，取 $U=2$ 或 $U=3$ 都满足要求．
$|u'^2-u'v'+v'^2|\leqslant u'^2+|u'v'|+v'^2\leqslant\dfrac{3}{4}$．$\alpha=\beta(U+V\omega)+(c+d\omega)(u'+v'\omega)$而且$\alpha-\beta(U+V\omega)\in Z[\omega]$．利用问题 41 的论证，得到$N[(c+d\omega)(u'+v'\omega)]\leqslant\dfrac{3}{4}N(c+d\omega)<N(c+d\omega)$.

这是 Z[ω] 中的除法算式，我们要用它来证明 Z[ω] 中的因子分解的唯一性．

54. (iii) 根据问题 53，$\alpha=\delta q+r$，其中 $N(r)<N(\delta)$．因为 $r=\alpha-(x_1\alpha+y_1\beta)q=(1-x_1q)\alpha+(-y_1q)\beta\in A$，而且 δ 在A 中有最小的正范数，所以 $N(r)=0$，从而 $r=0$，α 是 δ 的倍数．

在等距格上，集合 A 可以看作是一个等距子格，与其说它是由 1 构成不如说是由 δ 构成的．

若 $N(\gamma)=1$，则 $N(\gamma\delta)=N(\delta)$，所以在 Z[ω] 中至少有六个元素满足关于 gcd (α,β)的条件．若 $N(\delta)=N(\eta)$且 $\eta=\gamma\delta$，则 $N(\gamma)=1$，所以恰好有六个元素满足关于 gcd (α,β)的条件．

55. 因为 π 的因子仅有单位元，π，以及 π与单位元之积，而 π 又不整除 α，所以 gcd $(\pi,\alpha)=\delta=$一个单位元．

因为 1 是单位元的倍数，所以 $A=Z[\omega]$，而且存在 x 与 y，使得 $x\pi+y\alpha=1$，所以 $x\pi\beta+y\alpha\beta=\beta$．由于 $\pi\,|\,\alpha\beta$，所以 $\pi\,|\,\beta$.

56. 因为 $\pi_1\,|\,\pi_1\pi_2\cdots\pi_n$，所以由问题 55 知道 $\pi_1\,|\,\gamma_1$ 或者

$\pi_1 \mid \gamma_2 \cdots \gamma_m$. 若 $\pi_1 \mid \gamma_1$,则 $\pi_1 = \gamma_1 \times$ 单位元. 否则，可重复此推理 (最多 $m-1$ 次)，直至推出 $\pi_1 \mid \gamma_i$. 对 π_2 可用类似方法论证.假设由 $n-1$ 个素因子组成的乘积(不计单位元)是唯一的，那么,上面的第一部分的论证就是进行归纳推理的基础. 如果我们要叙述一个与 Z 中因数分解唯一性定理 (问题 1.58)相类似的定理，那么此处由单位元所引起的不便是不可避免的.

57. 是的，因为 $Z \subset Z[\omega]$.

58. 是的，取 $\alpha = x$, $\beta = y$, $\gamma = -z$.

59. 若 gcd $(x, y, z) = d$, 取 $\alpha = \dfrac{x}{d}$, $\beta = \dfrac{y}{d}$, $\gamma = \dfrac{z}{d}$.

60. $x^3 - 1 = (\alpha\lambda + 1)^3 - 1 = \alpha^3\lambda^3 + 3\alpha^2\lambda^2 + 3\alpha\lambda$.而 $3 = -\lambda^2$ ，所以 $x^3 - 1 = \alpha^3\lambda^3 - \alpha\lambda^3 - \alpha^2\lambda^4$. 由问题49 知道 $\alpha \equiv 0, 1, -1 \pmod{\lambda}$, 从而 $\alpha, \alpha+1, \alpha-1 \equiv 0 \pmod{\lambda}$. 于是 $\alpha(\alpha-1)\cdot(\alpha+1) \equiv 0 \pmod{\lambda}$, 从而 $(\alpha^3 - \alpha)\lambda^3 \equiv 0 \pmod{\lambda^4}$, 由此可得 $x^3 - 1 \equiv 0 \pmod{\lambda^4}$. 对于 $x = \alpha\lambda - 1$ 的情况，可用同法.

61. 若 $x, y, z \equiv \pm 1 \pmod{\lambda}$, 则由问题 60 知，$x^3, y^3, z^3 \equiv \pm 1 \pmod{\lambda^4}$, 于是 $x^3 + y^3 + z^3 \equiv \pm 3, \pm 1 \pmod{\lambda^4}$. 但是 $\lambda^4 = 9$, 因此，除非 x, y, z 中至少有一个含有因子 λ , 否则 $x^3 + y^3 + z^3 \equiv 0 \pmod{9}$ 是不可能的.

62. 若 $y \equiv 1 \pmod{\lambda}$, 则 $y^3 \equiv 1 \pmod{\lambda}$. 若 $y \equiv -1 \pmod{\lambda}$, 则 $y^3 \equiv -1 \pmod{\lambda}$. 因此 $y^3 + z^3 \equiv \pm 1 \pm 1 \pmod{\lambda}$. 但是 $y^3 + z^3 \equiv (-x)^3$ 及 $\lambda \mid x$, 所以 $y^3 + z^3 \equiv 0 \pmod{\lambda}$. 因此，$\{y^3, z^3\} \equiv \{1, -1\}$, 从而 $\{y, z\} \equiv \{1, -1\}$, 就是说 , y 与 z 对模 λ 不同余.

63. $y + \omega z = \alpha\lambda + 1 + \omega(\beta\lambda - 1) = \alpha\lambda + \beta\lambda + \omega^2\lambda$,

$\omega y + z = \omega(\alpha\lambda + 1) + \beta\lambda - 1 = \alpha\lambda + \beta\lambda - \omega^2\lambda$, $y + z = \alpha\lambda + \beta\lambda$. 因此 , $\lambda \mid y + \omega z, \omega y + z, y + z$.

若 $\delta\lambda \mid y+\omega z$，$y+z$，则 $\delta\lambda \mid (1-\omega)z$ 及 $\delta \mid \omega^2 z$，所以 δ 是单位元，或者 $\delta \mid z$．但 $\delta \mid y+z$，所以 $\delta \mid y$，z．

若 $\delta\lambda \mid \omega y+z$，$y+z$，则可做类似的论证．

若 $\delta\lambda \mid y+\omega z$，$\omega y+z$，则 $\delta\lambda \mid y+\omega z-\omega^2(\omega y+z)$，于是 $\delta\lambda \mid \lambda z$，$\delta \mid z$．因为 $\delta \mid \omega y+z$，所以 $\delta \mid \omega y$，因此 δ 是单位元，或者是 y 与 z 的公因子．

λ 不是 y 与 z 的公因子，所以 δ 没有因子 λ，因此，问题里的三个数中至多有一个数有因子 λ^2．

64．由问题 62 知，y，$z \equiv 1$，$-1 \pmod{\lambda}$，因此，由问题 61 知道 y^3，$z^3 \equiv 1, -1 \pmod{\lambda^4}$ 及 $-x^3 \equiv 0 \pmod{\lambda^4}$．因为 $x \equiv 0 \pmod{\lambda}$，所以有某个 γ 使 $x=\gamma\lambda$，因此 $x^3=\gamma^3\lambda^3$．但 $\lambda^4 \mid \gamma^3\lambda^3$，所以 $\lambda \mid \gamma^3$，而且，由于 γ 是素元，所以 $\lambda \mid \gamma$，$\lambda^2 \mid x$．

65．对任意的 y，z，有 $y^3+z^3=\omega^2(y+z)(\omega y+z)(y+\omega z)$．根据问题 59 和问题 62，不失一般性，可以假定问题 63 中的条件成立，以及 y 和 z 没有异于单位元的公因子，因此

$$\frac{\omega^2(y+z)}{\lambda}, \quad \frac{\omega y+z}{\lambda}, \quad \frac{y+\omega z}{\lambda}$$

中任何两个数都没有异于单位元的公因子，所以它们都是立方数，或立方数与单位元之积，且都是 $\left(-\dfrac{x}{\lambda}\right)^3$ 的因子．由问题 63 知，在

$$\frac{\omega^2(y+z)}{\lambda}, \quad \frac{\omega y+z}{\lambda}, \quad \frac{y+\omega z}{\lambda}$$

中至多有一个数有因子 λ，再因为这三个数之积是 $\left(-\dfrac{x}{\lambda}\right)^3$，所以它们的因子中 λ 的最高幂是 λ^{k-3}，这里的 λ^k 是整除 x^3 的 λ 的最高幂．

66．(i) $N(1+\omega)=N(-1-\omega)=1$，$N(1-\omega)=N(-1+\omega)=3$．$N(\lambda)=3$，所以 $N(\pi\lambda^3)=N(\pi)\cdot 27 \neq 1, 3$．

(ii) 由问题 60 得到

$$\alpha \equiv 0 \pmod{\lambda} \Rightarrow \alpha^3 \equiv 0 \pmod{\lambda^3},$$
$$\alpha \equiv 1 \pmod{\lambda} \Rightarrow \alpha^3 \equiv 1 \pmod{\lambda^3},$$
$$\alpha \equiv -1 \pmod{\lambda} \Rightarrow \alpha^3 \equiv -1 \pmod{\lambda^3}.$$

若$\lambda | \gamma$但λ不是α或β的因子，则由$\alpha^3+\omega\beta^3+\omega^2\gamma^3=0$推出$\pm 1 \pm \omega \equiv 0 \pmod{\lambda^3}$，这是不可能的(根据(i))。

若$\lambda | \alpha$，将等式乘以ω^2，然后作同样推理。

若$\lambda | \beta$，将等式乘以ω，然后作同样推理。

67. 因为三数之和是零及它们的乘积是一个立方数，所以，根据问题44，所给的等式具有$\alpha^3+\beta^3+\gamma^3=0$或$\alpha^3+\omega\beta^3+\omega^2\gamma^3=0$的形式。由问题65知，$\alpha^3$，$\beta^3$与$\gamma^3$中恰好有一个含有因子$\lambda$。于是，根据问题66，$\alpha^3+\omega\beta^3+\omega^2\gamma^3=0$是不可能的。这样，从一个形如$x^3+y^3=z^3$的等式出发，其中$x,y,z$无公因子，而且只有一个含因子$\lambda$，可以构造出另一个同样形状的等式，但在含因子$\lambda$的项中，$\lambda$的幂次降低了。重复这个构造过程，就可得到一个这种形状的等式，它的项都不含因子λ。这与问题61矛盾。这是使用Fermat递降法的又一个例子。

68. 给出的方程与$(x^m)^3+(y^m)^3+(z^m)^3=0$等价。若$m$是负数，$m=-n$，则它与$(y^nz^n)^3+(x^nz^n)^3=(x^ny^n)^3$等价。论断"对于$n>2$，不存在使$x^n+y^n=z^n$成立的非零整数$x,y,z$"即是著名的Fermat大定理，它至今还没有证明。为了证明这一结果对各种特殊的素数n成立，已经花费了大量的工作。

历史注记

一个按照一定规则来构造Pythagoras三元数组的方法早就为巴比伦人所知道了(公元前约1500年)。Euclid(公元前约300年)已经知道我们的公式(5.11)，而Diophantus(公元约200年)，则能证明这个公式给出了全部解。Fermat断言$x^4+y^4=z^4$没有整数解，而且，正如我们已经看到的，用他的递

降法给出了一个证明．Fermat 还宣布他有一个关于 $x^3+y^3=z^3$ 没有整数解的证明．1770 年，Euler 发表了对这个论断的一个长期被认为是完善的证明. C．F．Gauss 利用 1 的复立方根给出了另一个证明．

在一本 Diophantus 的书上的空白处，Fermat 写道："把一个立方分成两个立方，或者把一个双二次方 (即四次方)分成两个双二次方，一般地，把任何高于二次的幂分成两个同样次数的幂，都是不可能的；我已经发现了一个确实非凡的证明，但这空白太小，写不下．" 命题"当 $n>2$ 时，$x^n+y^n=z^n$ 没有整数解"是 Fermat 所宣布的结果中唯一还没有证明的结果，因此，称之为"Fermat 大定理"．如果能对所有奇素数 n 和 $n=4$ 证明 Fermat 大定理，那么就可以完全证明它了．为了扩大使 Fermat 定理成立的素数 n 的集合，Kummer 等人在十九世纪四十年代检验了有因式分解唯一性的域．他们对于某些复算术中不存在因式分解唯一性感到吃惊．直到现在，仅对 $n=4$ 及有限个素数 n 证明了 Fermat 大定理．

在 Bell (1962)的书中，转载了 Fermat 信件的一些有趣的摘编．在 Edward (1977)的书中，对有关"大定理"的工作，按照历史发展，作了详尽的介绍和研究．

第六章　平　方　和

二平方之和

1．在表 1.1 中,找出小于 100 且在表 5.1 中出现的那些数.

2．表 1.1 中的哪些列含有表 5.1 中的数,哪些列不含?

3．表 1.1 的哪些列含有表 5.1 中的奇素数,哪些列不含?

4．做一个模 4 的平方和表,并且证明形如 $4k+3$ 的数不可能是二平方之和.

5．把表 5.1 中小于 200 且有因数 3 的那些数列出来.对每个数找出能够整除它的 3 的最高次幂.

6．做一个模 3 的平方和表.若 $x^2+y^2\equiv 0 \pmod 3$,对 x 和 y 能做什么推断?对 x^2+y^2 呢?

7．把表 5.1 中小于 200 且有因数 7 的那些数列出来.对每个数找出能够整除它的 7 的最高次幂.

8．做一个模 7 的平方和表.若 $x^2+y^2\equiv 0 \pmod 7$,对 x 和 y 能做什么推断?对 x^2+y^2 呢?

9．假设数素 p $(\neq 2)$ 能整除形如 x^2+y^2 的一个数;于是 $x^2+y^2\equiv 0 \pmod p$;那么,若 $y\not\equiv 0 \pmod p$,则存在整数 a,使得 $ay\equiv 1 \pmod p$,从而有 $(ax)^2+1\equiv 0 \pmod p$.因此,ax 是 $\mathbf{M}_p$ 中的4阶元素.根据Lagrange关于子群的定理,对于 p 能知道些什么?(与问题 4.18 及问题 4.19 做比较).

10．试陈述问题9 的逆否命题,以推广问题 6 与问题8.

11．当 $p=2$ 时,问题 9 的结论是否正确?

12．若 x^2+y^2 被27 整除,是否必被 81 整除?推广你的论证.

13．考察表5.1 中的数的素因数分解,从而提出一个关于哪些

正整数可以表为两个平方数之和的猜想.

14. 在表 5.1 中找出三个数,它们都在第一列之外至少出现二次.把每个数表示成表中的二数之积.利用形如

$$13=2^2+3^2=(2+3i)(2-3i)$$

的复数因子分解,把你原来的三个数都表示为四个复数之积.通过改变乘积中的四个复数的次序,为你找到的三个形如 $a^2+b^2=c^2+d^2$ 的等式的例子提出一个理论根据.

15. 若 a 和 b 是整数,称形如 $a+ib$ 的复数为Gauss整数.

将 a^2+b^2 分解为 Gauss 整数之积.设 a, b, c, d, 是整数,把 $(a^2+b^2)(c^2+d^2)$表成四个 Gauss 整数之积.重排这四个因数,使前面两个是后面两个的共轭复数.把前两个相乘得到一个 Gauss 整数.后两个相乘也得到一个Gauss 整数.用这样的方法所得的两个 Gauss 整数是否为共轭复数?

将 $(a^2+b^2)(c^2+d^2)$表为两个平方数之和.

16. 如何利用上题最后得到的恒等式来证明你在问题 13 中所提出的部分猜想?

17. 你在问题 13 中所提出的猜想还有哪些部分没有证明?

18. 求出表 5.1 第二列中所有数的素因数.

19. 利用问题 4.22 来判断,是否只要把表 5.1 延伸下去,同余于1 (mod 4)的素数就一定是第二列中某数的因数?

20. 将表 5.1 中形如 n^2+1 的素数列出来.

21. 将表 5.1 中形如 n^2+1 且是某个奇素数二倍的数列出来.

22. 按照下面的方法,由等式 $35^2+1=2\cdot613$ 可以导出 613 表为两个平方之和的表达式:

$$(35^2+1)(1^2+1^2)=613\cdot2^2$$

$$\Rightarrow\quad (35+1)^2+(35-1)^2=613\cdot2^2\quad(\text{由问题 15})$$

$$\Rightarrow\quad 36^2+34^2=613\cdot2^2$$

$$\Rightarrow\quad 18^2+17^2=613.$$

将这个方法用于你在问题 21 中所得到的各个等式,把 13,41,61,113,181 及 313 表为二平方之和.

已知$79^2+1=2\cdot3121$与$85^2+1=2\cdot3613$,将素数 3121 与 3613 表为二平方之和.

23. 已知

$$42^2+1=5\cdot353,$$
$$48^2+1=5\cdot461,$$
$$52^2+1=5\cdot541,$$
$$58^2+1=5\cdot673,$$

改进上题方法,将 353,461,541,673表示为二平方之和.

24. 改进上题方法,利用$7^2+4^2=5\cdot13$与$9^2+2^2=17\cdot5$将13与17表示为二平方之和.

25. 已知 $33^2+1=10\cdot109$与$67^2+1=10\cdot449$.利用问题 22 与问题 24 的方法将 109 与 449 表示为二平方之和.尽管利用$3^2+1=10$可以一步就做出来,但是,若分两步来做,即先去掉因数 2,再去掉因数 5,却更有启发性.

26. 对等式$11^2+13^2=10\cdot29$应用上题的"两步方法",求29 的二平方和表示式.

27. 已知 $34^2+1=13\cdot89$,求整数x,y,使得$(34^2+1)(x^2+y^2)=13^2\cdot89$,而且$34x+y$及$34y-x$都被 13 整除.由此导出 89 的二平方和表示式.

28. 设$p=x^2+y^2$是素数且$n^2+1=pk$,证明$nx\equiv\pm y \pmod p$,再利用等式

$$\begin{aligned}(n^2+1)(x^2+y^2)&=(nx+y)^2+(ny-x)^2\\&=(nx-y)^2+(ny+x)^2\end{aligned}$$

导出k的二平方和表示式.

29. 已知 $113^2+22^2=457\cdot29$,求整数x,y,使得$(113^2+22^2)(x^2+y^2)=457\cdot29^2$,而且$113x+22y$与$113y-22x$都被 29 整除.由此导出 457的二平方和表示式.

30. 设$p=x^2+y^2$是素数且$m^2+n^2=pk$,证明$mx\equiv\pm ny \pmod p$,再利用等式

$$(m^2+n^2)(x^2+y^2)=(mx+ny)^2+(my-nx)^2$$
$$=(mx-ny)^2+(my+nx)^2$$

导出 k 的二平方和表示式.

31. m^2+1 能有多少个大于 m 的素因数?

32. 设当 $n<m$ 时,n^2+1 的每一个素因数都可表示为两个平方数之和,证明 m^2+1 的每一个小于 m 的素因数都可表示为二平方之和.

重复利用问题 30 ,并注意到问题 31 ,证明 m^2+1 的素因数都可以表示为二平方之和.

33. 利用问题 32 及归纳法,证明形如 n^2+1 的数的素因数都可以表示为二平方之和.证明每个同余于 1 (mod 4)的素数都可以表示为二平方之和.

34. 将可以表示为二平方之和的整数做一个完整的分类.

35. 有没有素数在表 5.1 中出现两次?

36. 设素数 $p=a^2+b^2=c^2+d^2$ 且 $p|n^2+1$,

(i) 证明 $na\equiv \pm b$ 及 $nc\equiv \pm d \pmod p$,

(ii) 利用等式

$$p^2=(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$$
$$=(ac-bd)^2+(ad+bc)^2,$$

证明在右端的两个表达式中,必有一个的两项都被 p 整除,从而必有一项是 0.

证明 $\{a^2,b^2\}=\{c^2,d^2\}$.

四平方之和

37. 将 1 到20 的整数表示成至多四个平方数之和.

38. 设 a,b,c,d 是整数,且规定

$$i^2=j^2=k^2=-1, ij=-ji=k, jk=-kj=i, ki=-ik=j,$$

我们定义四元数 $\alpha=a+bi+cj+dk$ 以及它的共轭四元数

$\overline{\alpha}=a-bi-cj-dk$. 假定与 i,j,k 在一起的整数是与它们相乘，而且通常的分配律成立，求乘积 $\alpha\overline{\alpha}$.

对任意的两个四元数 α,β，证明 $\overline{\beta\alpha}=\overline{\alpha}\,\overline{\beta}$.

39. 设 a,b,c,d,x,y,z,t 是整数，把

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)$$

表示成四个四元数之积，再表示成两个共轭四元数之积.

证明：如果两个整数都可以表示成四个平方数之和，则它们的乘积也可以表示成四个平方数之和.

40. 在问题 34 中已经知道，任何正整数，只要它的素因数分解式中不含有同余于 3 (mod 4)的素数 p 的奇次幂，就可以表为二平方数之和. 为了证明每一个正整数能表示成四个平方数之和，还需要再证明什么？(Lagrange 四平方数定理).

41. 设 p 是奇素数，那么 $\mathbf{Z}_p$ 中有多少个平方数？在集合 $\{-(x^2)|x\in\mathbf{Z}_p\}$ 与 $\{x^2+1|x\in\mathbf{Z}_p\}$ 中各有多少个不同的元素？

证明这两个集合相交，及存在整数 x,y，使得 $x^2+y^2+1\equiv 0 \pmod p$.

42. 设 p 是奇素数，是否必有整数 x,y，$0\leqslant x,y<\frac{1}{2}p$，使得 $x^2+y^2+1\equiv 0 \pmod p$？

证明存在整数 a,b,c,d，使得 $a^2+b^2+c^2+d^2=mp$，其中 $m<p$.

43. $2^2+4^2+6^2+8^2=120$,

$1^2+2^2+3^2+4^2=30$,

$1^2+3^2+5^2+7^2=84$.

若 a,b,c,d 是整数，$a^2+b^2+c^2+d^2$ 是偶数，那么 a,b,c,d 中能有几个奇数？

44. 若 a 与 b 的奇偶性相同，那么关于 $a+b$ 与 $a-b$ 能说些什么？

45. 设 $$\left(\frac{a+b}{2}\right)^2+\left(\frac{a-b}{2}\right)^2+\left(\frac{c+d}{2}\right)^2+\left(\frac{c-d}{2}\right)^2$$
$$=k(a^2+b^2+c^2+d^2),$$

求 k 值.

46. $1^2+3^2+5^2+7^2=84$.

利用问题 45,将 42 表示成四平方之和,再将 21 表示成四平方之和.

47. 设 a,b,c,d 是整数且

$$a^2+b^2+c^2+d^2=mp,$$

其中 m 是偶数,证明存在 p 的一个倍数,它比 mp 小,且可表示成四平方之和.

48. $1^2+2^2+3^2+5^2=39=3\cdot 13$.

若选取 $x\equiv 1 \pmod 3$, $y\equiv 2 \pmod 3$, $z\equiv 3 \pmod 3$ 及 $t\equiv 5 \pmod 3$,证明

$$x^2+y^2+z^2+t^2,$$
$$x+2y+3z+5t,$$
$$y-2x-3t+5z,$$
$$z+2t-3x-5y$$

与

$$t-2z+3y-5x$$

都被 3 整除. 取 x,y,z,t 是绝对值最小的数,并将乘积

$$(1^2+2^2+3^2+5^2)(x^2+y^2+z^2+t^2)$$

表示成四平方之和. 由此推出 13 的四平方和表示式.

49. $1^2+1^2+2^2+17^2=295=5\cdot 59$.

取 x,y,z,t 满足 $x\equiv 1 \pmod 5$, $y\equiv 1 \pmod 5$, $z\equiv 2 \pmod 5$, $t\equiv 17 \pmod 5$,且有最小的绝对值,并将给出的等式乘以 $x^2+y^2+z^2+t^2$,由此推出 59 的四平方和表示式.

50. 设 a,b,c,d 是整数且

$$a^2+b^2+c^2+d^2=mp,$$

其中 $m>1$ 是奇数,又设 x,y,z,t 满足 $x\equiv a \pmod m$, $y\equiv b \pmod m$, $z\equiv c \pmod m$, $t\equiv d \pmod m$,且有最小的绝对值,证明

$$x^2+y^2+z^2+t^2<m^2,$$

以及

$$x^2+y^2+z^2+t^2,$$
$$ax+by+cz+dt,$$
$$ay-bx-ct+dz,$$
$$az+bt-cx-dy$$

与

$$at-bz+cy-dx$$

都被 m 整除.

证明,对于某个整数 m',$0<m'<m$,$m'p$ 可以表示成四平方之和.

51. 设 p 是奇素数,利用问题 41,问题 47 及问题 50 证明:在使 mp 可以表示成四平方之和的整数 m 中,大于 1 的都不是最小的,因此,p 可以表示成四平方之和.

52. 利用问题 39,问题51 以及等式 $0^2+0^2+1^2+1^2=2$,证明正整数都可以表示成四平方之和.

三平方之和

53. 试将从 1 到20 的整数表示成三个平方数之和.

54. 做一个模 8 的平方和表.

能否找到整数 x,y,z,使得 $x^2+y^2+z^2\equiv 7 \pmod 8$?

若 $x^2+y^2+z^2\equiv 0 \pmod 4$,对于 x^2,y^2 及 z^2 能说些什么?

若 $4m$ 是三平方之和,证明 m 也是三平方之和.

证明:不存在非负整数 h,k,使得 $4^h(8k+7)$能表示成三平方之和.

注记与答案

参考书见书目:

Bolker (1970),Davenport (1978),Ore (1948), Shanks (1978).

1. 0,4,8,16,20,32,36,40,52,64,68,72,80 $\equiv 0 \pmod 4$.

1,5,9,13,17,25,29,37,41,45,49,61,65,73,81,85,89,97 $\equiv 1 \pmod 4$.

10,18,26,34,50,58,74,82,90,98 $\equiv 2 \pmod 4$.

2. 除去同余于3 (mod 4)的那些数.

3. 只有同余于1 (mod 4)的那些数.

4. 此处及本章中,$x^2 = x^2 + 0^2$ 算做二平方之和.

.	0	1	2	3
0	0	1	0	1
1	1	2	1	2
2	0	1	0	1
3	1	2	1	2

5. $9, 18 = 9\cdot 2$, $36 = 9\cdot 4$, $45 = 9\cdot 5$, $72 = 9\cdot 8$, 81, $90 = 9\cdot 10$, $117 = 9\cdot 13$, $144 = 9\cdot 16$, $153 = 9\cdot 17$, $162 = 81\cdot 2$, $180 = 9\cdot 20$.

6.

	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

$x^2 + y^2 \equiv 0 \pmod 3$

$\Rightarrow x \equiv y \equiv 0 \pmod 3$

$\Rightarrow x^2 + y^2 \equiv 0 \pmod 9$.

7. 49, $98 = 49\cdot 2$, $196 = 49\cdot 4$.

8. $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$, $6^2 \equiv 1 \pmod 7$.

0	1	2	4
1	2	3	5
2	3	4	6
4	5	6	1

$x^2 + y^2 \equiv 0 \pmod 7$

$\Rightarrow x \equiv y \equiv 0 \pmod 7$

$\Rightarrow x^2 + y^2 \equiv 0 \pmod{49}$.

9. 若 $\mathbf{M}_p$ 有一个4 阶元素,则$4 | p-1$,$p \equiv 1 \pmod 4$.

10. 若 $p\equiv 3 \pmod 4$,则

$$x^2+y^2\equiv 0 \pmod p$$
$$\Rightarrow x\equiv y\equiv 0 \pmod p$$
$$\Rightarrow x^2+y^2\equiv 0 \pmod{p^2}.$$

11. 因为 $1\equiv -1 \pmod 2$,所以由 $(ax)^2+1\equiv 0 \pmod 2$不能推出ax在$\mathbf{M}_2$中是4阶.由 $x^2+y^2\equiv 0 \pmod 2$能推出 x 与 y 同为奇数或偶数.在这一点上,2 和同余于 $1 \pmod 4$的素数相似,而和同余于 $3 \pmod 4$的素数不相似.

12. 因为 $27|x^2+y^2\Rightarrow x^2+y^2\equiv 0 \pmod 3$,所以,由问题 6 得出 $x=3x'$,$y=3y'$.因此,$x^2+y^2=9(x'^2+y'^2)$,$3|x'^2+y'^2$.由问题 6,$x'=3x''$,$y'=3y''$,于是 $x^2+y^2=81(x''^2+y''^2)$.利用与问题 10 相似的论证推出,如果素数 $p|x^2+y^2$ 而且 $p\equiv 3 \pmod 4$,则整除 x^2+y^2 的 p 的最高次数是偶数.

13. 形如 x^2+y^2的数的素因数分解式中,同余于 $3 \pmod 4$ 的素数 p 的指数是偶数,另外的素数的指数则可以是任意的.

14. $50=5\cdot 10=(2^2+1^2)(3^2+1^2)$
$\quad =(2+i)(2-i)(3+i)(3-i)$

$[(2+i)(3+i)][(2-i)(3-i)]=(5+5i)(5-5i)=5^2+5^2$

$[(2+i)(3-i)][(2-i)(3+i)]=(7+i)(7-i)=7^2+1^2$

$65=5\cdot 13=(2^2+1^2)(2^2+3^2)$
$\quad =(2+i)(2-i)(2+3i)(2-3i)$

$[(2+i)(2+3i)][(2-i)(2-3i)]=(1+8i)(1-8i)=1^2+8^2$

$[(2-i)(2+3i)][(2+i)(2-3i)]=(7+4i)(7-4i)=7^2+4^2$

$85=5\cdot 17=(2^2+1^2)(4^2+1^2)$
$\quad =(2+i)(2-i)(4+i)(4-i)$

$[(2+i)(4+i)][(2-i)(4-i)]=(7+6i)(7-6i)=7^2+6^2$

$[(2+i)(4-i)][(2-i)(4+i)]=(9+2i)(9-2i)=9^2+2^2$

15. 用 $\mathbf{Z}[i]$ 表示全体 Gauss 整数，与问题 5.56 中对$\mathbf{Z}[w]$ 所证明的一样，在 $\mathbf{Z}[i]$ 中也有唯一因子分解定理成立. 这可通过定义范数$N(a+ib)=a^2+b^2$ 来证明，但是，我们这里不用这个定理.

$$a^2+b^2=(a+bi)(a-bi)$$

$$(a^2+b^2)(c^2+d^2)=(a+bi)(a-bi)(c+di)(c-di)$$

$$[(a+bi)(c+di)(a-bi)(c-di)]$$

$$=[(ac-bd)+(ad+bc)i][(ac-bd)-(ad+bc)i]$$

$$=(ac-bd)^2+(ad+bc)^2,$$

而且

$$[(a+bi)(c-di)][(a-bi)(c+di)]$$

$$=[(ac+bd)-(ad-bc)i][(ac+bd)+(ad-bc)i]$$

$$=(ac+bd)^2+(ad-bc)^2.$$

16. 问题15中的恒等式表明，由可以表为二平方之和的整数所组成的集合对乘法是封闭的. 因此，每个正整数，若它的素因数分解式中的指数都是偶数，则一定可以表示成二平方之和，这是因为这样的整数都是平方数，而且显然有 $x^2=x^2+0^2$.

17. 还需要证明：每一个同余于 1 (mod 4)的素数都可以表示为二平方之和.

18. 根据问题4.24，只需考察同余于 1 (mod 4)的素因数，再根据问题 1.47，只需研究不超过 41 的这种素数. 或利用 Hubbard (1975)的书.

见注记 20 与注记 21. 此外，有下面的结果：

两个素因数：$8^2+1=5\cdot13$，$12^2+1=5\cdot29$，$22^2+1=5\cdot97$，
$28^2+1=5\cdot157$，　$30^2+1=17\cdot53$，　$34^2+1=13\cdot89$，
$42^2+1=5\cdot353$，　$44^2+1=13\cdot149$，　$46^2+1=29\cdot73$，
$48^2+1=5\cdot461$，　$50^2+1=41\cdot61$.

三个素因数：$13^2+1=2\cdot5\cdot17$，　$17^2+1=2\cdot5\cdot29$，
$21^2+1=2\cdot13\cdot17$，　$23^2+1=2\cdot5\cdot23$，　$27^2+1=2\cdot5\cdot73$，
$31^2+1=2\cdot13\cdot37$，　$33^2+1=2\cdot5\cdot109$，　$37^2+1=2\cdot5\cdot137$.

三个素因数，其中有一个重复：$7^2+1=2\cdot 5^2$, $18^2+1=5^2\cdot 13$, $32^2+1=5^2\cdot 41$, $38^2+1=5\cdot 17^2$, $41^2+1=2\cdot 29^2$.

四个素因数：$43^2+1=2\cdot 5^2\cdot 37$, $47^2+1=2\cdot 5\cdot 13\cdot 17$.

19. 根据问题 4.18 或问题 4.29，对于任一素数 $p\equiv 1 \pmod 4$，-1 是对模 p 的二次剩余，所以存在整数 n，使得 $n^2\equiv -1 \pmod p$ 及 $p|n^2+1$.

20. 素数.

$1^2+1=2$, $2^2+1=5$, $4^2+1=17$, $6^2+1=37$,
$10^2+1=101$, $14^2+1=197$, $16^2+1=257$, $20^2+1=401$,
$24^2+1=577$, $26^2+1=677$, $36^2+1=1297$, $40^2+1=1601$.

21. 素数乘 2.

$3^2+1=2\cdot 5$, $5^2+1=2\cdot 13$, $9^2+1=2\cdot 41$, $11^2+1=2\cdot 61$,
$15^2+1=2\cdot 113$, $19^2+1=2\cdot 181$, $25^2+1=2\cdot 313$,
$29^2+1=2\cdot 421$, $35^2+1=2\cdot 613$, $39^2+1=2\cdot 761$,
$45^2+1=2\cdot 1013$, $49^2+1=2\cdot 1201$.

22. $5^2+1=2\cdot 13\Rightarrow 6^2+4^2=2^2\cdot 13\Rightarrow 3^2+2^2=13$.

$9^2+1=2\cdot 41\Rightarrow 10^2+8^2=2^2\cdot 41\Rightarrow 5^2+4^2=41$.

$11^2+1=2\cdot 61\Rightarrow 12^2+10^2=2^2\cdot 61\Rightarrow 6^2+5^2=61$.

$15^2+1=2\cdot 113\Rightarrow 16^2+14^2=2^2\cdot 113\Rightarrow 8^2+7^2=113$.

$19^2+1=2\cdot 181\Rightarrow 20^2+18^2=2^2\cdot 181\Rightarrow 10^2+9^2=181$.

$25^2+1=2\cdot 313\Rightarrow 26^2+24^2=2^2\cdot 313\Rightarrow 13^2+12^2=313$.

$79^2+1=2\cdot 3121\Rightarrow 80^2+78^2=2^2\cdot 3121\Rightarrow 40^2+39^2=3121$.

$85^2+1=2\cdot 3613\Rightarrow 86^2+84^2=2^2\cdot 3613\Rightarrow 43^2+42^2=3613$.

23. $42^2+1=5\cdot 353\Rightarrow (42^2+1)(2^2+1)=5^2\cdot 353$

$$\Rightarrow (42+1\cdot 1)^2+(42\cdot 1-1\cdot 2)^2=5^2\cdot 353$$

$$\Rightarrow 85^2+40^2=5^2\cdot 353$$

$$\Rightarrow 17^2+8^2=353.$$

$$48^2+1=5\cdot 461 \Rightarrow (48^2+1)(2^2+1)=5^2\cdot 461$$
$$\Rightarrow (48\cdot 2-1\cdot 1)^2+(48\cdot 1+1\cdot 2)^2 = 5^2\cdot 461$$
$$\Rightarrow 95^2+50^2=5^2\cdot 461$$
$$\Rightarrow 19^2+10^2=461.$$
$$52^2+1=5\cdot 541 \Rightarrow (52^2+1)(2^2+1)=5^2\cdot 541$$
$$\Rightarrow 105^2+50^2=5^2\cdot 541$$
$$\Rightarrow 21^2+10^2=541.$$
$$58^2+1=5\cdot 673 \Rightarrow (58^2+1)(2^2+1)=5^2\cdot 673$$
$$\Rightarrow 60^2+115^2=5^2\cdot 673$$
$$\Rightarrow 12^2+23^2=673.$$

24. $$7^2+4^2=5\cdot 13 \Rightarrow (7^2+4^2)(2^2+1)=5^2\cdot 13$$
$$\Rightarrow (7\cdot 2-4\cdot 1)^2+(7\cdot 1+4\cdot 2)^2 = 5^2\cdot 13$$
$$\Rightarrow 10^2+15^2=5^2\cdot 13$$
$$\Rightarrow 2^2+3^2=13.$$
$$9^2+2^2=5\cdot 17 \Rightarrow (9^2+2^2)(2^2+1)=5^2\cdot 17$$
$$\Rightarrow (9\cdot 2+2\cdot 1)^2+(9\cdot 1-2\cdot 2)^2 = 5^2\cdot 17$$
$$\Rightarrow 20^2+5^2=5^2\cdot 17$$
$$\Rightarrow 4^2+1^2=17.$$

25. $$33^2+1=2\cdot 5\cdot 109 \Rightarrow 34^2+32^2=2^2\cdot 5\cdot 109$$
$$\Rightarrow 17^2+16^2=5\cdot 109$$
$$\Rightarrow (17^2+16^2)(2^2+1)=5^2\cdot 109$$
$$\Rightarrow (17\cdot 2+16\cdot 1)^2 + (17\cdot 1-16\cdot 2)^2=5^2\cdot 109$$
$$\Rightarrow 50^2+15^2=5^2\cdot 109$$
$$\Rightarrow 10^2+3^2=109.$$
$$67^2+1=2\cdot 5\cdot 449 \Rightarrow 68^2+66^2=2^2\cdot 5\cdot 449$$
$$\Rightarrow 34^2+33^2=5\cdot 449$$

$$\Rightarrow (34^2+33^2)(2^2+1)=5^2\cdot 449$$
$$\Rightarrow (34\cdot 2-33\cdot 1)^2$$
$$+(34\cdot 1+33\cdot 2)^2=5^2\cdot 449$$
$$\Rightarrow 35^2+100^2=5^2\cdot 449$$
$$\Rightarrow 7^2+20^2=449.$$

26． $11^2+13^2=2\cdot 5\cdot 29\Rightarrow 24^2+2^2=2^2\cdot 5\cdot 29$
$$\Rightarrow 12^2+1^2=5\cdot 29$$
$$\Rightarrow (12^2+1^2)(2^2+1^2)=5^2\cdot 29$$
$$\Rightarrow (12\cdot 2+1\cdot 1)^2+(12\cdot 1-2\cdot 1)^2$$
$$=5^2\cdot 29$$
$$\Rightarrow 25^2+10^2=5^2\cdot 29$$
$$\Rightarrow 5^2+2^2=29.$$

27．因为$x^2+y^2=13$，所以 $x,y=\pm 2,\pm 3$．事实上，$(x,y)=(2,-3),(-2,3),(3,2)$或$(-3,-2)$．

$(34^2+1)(2^2+3^2)=13^2\cdot 89\Rightarrow (34\cdot 2-1\cdot 3)^2+(34\cdot 3+1\cdot 2)^2$
$$=13^2\cdot 89$$
$$\Rightarrow 65^2+104^2=13^2\cdot 89$$
$$\Rightarrow 5^2+8^2=89.$$

28． $n^2\equiv -1$ 及 $x^2\equiv -y^2\Rightarrow n^2x^2\equiv y^2$，所以 $nx\equiv \pm y \pmod p$．

若 $nx\equiv y$，则 $ny\equiv -x$ 且 $p\mid nx-y,ny+x$，所以

$$\left(\frac{nx-y}{p}\right)^2+\left(\frac{ny+x}{p}\right)^2=k.$$

当$nx\equiv -y \pmod p$时，论证是类似的．

29． 因为$x^2+y^2=29$，$y=\pm 2,\pm 5$．

$(x,y)=(2,-5),(-2,5),(5,2)$或$(-5,-2)$．

$(113^2+22^2)(2^2+5^2)=29^2\cdot 457$
$$\Rightarrow (113\cdot 2-22\cdot 5)^2+(113\cdot 5+22\cdot 2)^2=29^2\cdot 457$$
$$\Rightarrow 116^2+609^2=29^2\cdot 457$$

$\Rightarrow 4^2+21^2=457$.

30. $m^2=-n^2$ 及 $x^2\equiv -y^2\Rightarrow m^2x^2\equiv n^2y^2$，所以$mx\equiv \pm ny$，$(\bmod p)$.若 $mx\equiv ny$，则 $mny\equiv m^2x\equiv -n^2x$，所以 $my\equiv -nx$ $(\bmod p)$，及 $p\mid mx-ny$，$my+nx$，因此

$$\left(\frac{mx-ny}{p}\right)^2+\left(\frac{my+nx}{p}\right)^2=k.$$

当$mx\equiv -ny$ $(\bmod p)$时，论证是类似的.

31. 设$p,q\mid m^2+1$且$p,q\geqslant m+1$，则$p,q\geqslant m^2+2m+1>m^2+1$，所以 m^2+1 至多有一个大于 m 的素因数.

32. 若$p\mid m^2+1$且$p<m$，则$p\mid (m-p)^2+1$，而且由假设可知 p 是二平方之和.

设 $m^2+1=p_1p_2\ldots p_n$，其中p_i 是素数，但可以相同.由问题31知，至多有一个 $p_i>m$.设$p_n>m$.根据假设，另外的素因数都是二平方之和，因此，反复利用问题 30 可推出

$$\frac{m^2+1}{p_1},\ \frac{m^2+1}{p_1p_2},\ \cdots,\ \frac{m^2+1}{p_1p_2\cdots p_{n-1}}$$

都是二平方之和.最后一数就是 p_n.

33. $2=1^2+1^2$ 是二平方之和，这是对 m 实行归纳法的第一步.归纳步骤见问题 32.因此，形如 n^2+1 的数的素因数都可表为二平方之和.由问题19 知，它们恰好就是全部同余于1 $(\bmod 4)$ 的素数以及素数 2.

34. 由问题 33 知，素数 2 以及每一个同余于1 $(\bmod 4)$的素数可以表示成二平方之和，因此，由问题 15 得出，二平方之和的数的素因数分解式中，这种素数的指数可以是任意的，而且根据问题 10，同余于 3 $(\bmod 4)$的素数在分解式中只能有偶指数.

35. 没有.

36. $n^2\equiv -1$，$a^2\equiv -b^2$，$c^2\equiv -d^2$，$\Rightarrow$ $a^2n^2\equiv b^2$ 且 $c^2n^2\equiv d^2$ $(\bmod p)$.因此，$an\equiv \pm b$，$cn\equiv \pm d$ $(\bmod p)$.

若$an\equiv b$ 且$cn\equiv d$ 或 $an\equiv -b$且$cn\equiv -d$ $(\bmod p)$，则

$ac+bd\equiv ac\ (1+n^2)\equiv 0$ 且 $ad-bc\equiv \pm ac\ (n-n)\equiv 0 \pmod{p}$. 因此,等式

$$p^2=(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$$

的两边可用 p^2 整除.这给出了数 1 的二平方和表示式,因此其中必有一项为 0. 若 $ad=bc$,则

$$d^2(a^2+b^2)=b^2c^2+d^2b^2=b^2(c^2+d^2),$$

于是 $b^2=d^2$.符号交错的情况可同样证明.对于数组$\{a^2,b^2\}$的唯一性,利用 Gauss 整数中的因子分解唯一性可以给出一个较简单的证明.

本题所证明的就是:如果一个素数可表为二平方之和,则只能有一种表示法.

37. 一个平方:1,4,9,16.

二个平方:2,5,8,10,13,17,18,20.

三个平方:3,6,11,12,14,19.

四个平方:7,15.

38.

$$\begin{aligned}(a+bi+cj+dk)(a-bi-cj-dk)\\ &=a^2-abi-acj-adk\\ &+abi+b^2-bck+bdj\\ &+acj+bck+c^2-cdi\\ &+adk-bdj+cdi+d^2=a^2+b^2+c^2+d^2.\end{aligned}$$

$$\begin{aligned}\alpha\beta&=(a+bi+cj+dk)(x+yi+zj+tk)\\ &=ax+ayi+azj+atk\\ &\quad+bxi-by+bzk-btj\\ &\quad+cxj-cyk-cz+cti\\ &\quad+dxk+dyj-dzi-dt\\ &=(ax-by-cz-dt)\\ &\quad+i(ay+bx+ct-dz)\\ &\quad+j(az-bt+cx+dy)\\ &\quad+k(at+bz-cy+dx)\end{aligned}$$

因此

$$\overline{\beta\alpha}=(ax-by-cz-dt)$$
$$-i(xb+ya+zd-tc)$$
$$-j(xc-yd+za+tb)$$
$$-k(xd+yc-zb+ta)=\overline{\alpha}\,\overline{\beta}.$$

39. 使用问题 38 中的 α,β,有

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)=\alpha\overline{\alpha}\beta\overline{\beta}.$$

$\beta\overline{\beta}$ 是实数,所以可与$\overline{\alpha}$ 交换,故

$$\alpha\overline{\alpha}\beta\overline{\beta}=\alpha\beta\overline{\beta}\,\overline{\alpha}=\alpha\beta\overline{\alpha\beta}$$
$$=(ax-by-cz-dt)^2+(ay+bx+ct-dz)^2$$
$$+(az-bt+cx+dy)^2+(at+bz-cy+dx)^2$$

是四平方之和.

40. 若每一个同余于 3 (mod 4)的素数可以表示成四平方之和,那么定理就证明了.

41. $\mathbf{Z}_p$ 中有 $\frac{1}{2}(p-1)$ 个二次剩余. 0 也是平方数. 因此 $\mathbf{Z}_p$ 中共有$\frac{1}{2}(p+1)$个平方数.

这两个集合中的每一个都有 $\mathbf{Z}_p$ 的 $\frac{1}{2}(p+1)$个元素,而且 $\frac{1}{2}(p+1)+\frac{1}{2}(p+1)=p+1$大于 $\mathbf{Z}_p$ 中不相同的元素个数.

42. $x^2\equiv(p-x)^2 \pmod p$,所以,如果 $0\leqslant x<p$,则 $x<\frac{1}{2}p$ 或 $p-x<\frac{1}{2}p$,因此存在整数$x,y,0\leqslant x,y<\frac{1}{2}p$,使得 $x^2+y^2+1^2+0^2\equiv 0 \pmod p$, $x^2+y^2+1^2+0^2=mp$. 但是$x^2,y^2<\left(\frac{1}{2}p\right)^2$, 因此当$p>2$ 时,$x^2+y^2+1<\frac{1}{2}p^2+1<p^2$, 所以 $m<p$.

这一基本结果的另一证明,可用问题 3.82 得到.

43. 有 0,2 或 4 个奇数. $a^2\equiv a \pmod 2$.

44. $a+b$ 与 $a-b$ 都是偶数.

45. $k=\frac{1}{2}$.

46. $1^2+3^2+5^2+7^2=84$,所以

$2^2+1^2+6^2+1^2=\frac{1}{2}\cdot 84=42$ (由问题45),

$1^2+1^2+2^2+6^2=42$,

$1^2+0^2+4^2+2^2=\frac{1}{2}\cdot 42$ (由问题45),

$0^2+1^2+2^2+4^2=21$.

47. 若 mp 是偶数,则a,b,c,d 是由两对奇偶性相同的数组成. 若 a 与b,c 与 d 有相同的奇偶性,则可利用问题 45 将 $\frac{1}{2}mp$ 表成四平方之和.

48. $1^2+2^2+3^2+5^2\equiv 0 \pmod 3$, 所以$1x+2y+3z+5t\equiv 0 \pmod 3$ 且 $x^2+y^2+z^2+t^2\equiv 0 \pmod 3$.

由 $1y\equiv 2x$ 及 $3t\equiv 5z \pmod 3$推出第三个式子被3整除.

由 $1z\equiv 3x$ 及 $2t\equiv 5y \pmod 3$推出关于第四个式子的结论.

由 $1t\equiv 5x$ 及 $2z\equiv 3y \pmod 3$推出关于第五个式子的结论.

取 $x=1,y=-1,z=0,t=-1$,利用问题 39 中的恒等式(改变 b,c,d 的符号)得到

$$(1^2+2^2+3^2+5^2)(1^2+(-1)^2+0^2+(-1)^2)$$

$$=(1-2+0-5)^2+(-1-2+3+0)^2+(0-2-3+5)^2$$

$$+(-1-0-3-5)^2,$$

即是 $3^2\cdot 13=6^2+0^2+0^2+9^2$, $13=2^2+0^2+0^2+3^2$.

49. 取 $x=1,y=1,z=2,t=2$.

$$(1^2+1^2+2^2+17^2)(1^2+1^2+2^2+2^2)$$

$$=(1+1+4+34)^2+(1-1-4+34)^2$$

$$+(2+2-2-17)^2+(2-2+2-17)^2,$$

即是 $$2\cdot 5^2\cdot 59=40^2+30^2+15^2+15^2,$$

$$2\cdot 59=8^2+6^2+3^2+3^2,$$

所以 $$59=7^2+1^2+3^2+0^2.$$

50. 因为 $$a^2+b^2+c^2+d^2\equiv 0 \pmod m,$$

所以 $$ax+by+cz+dt\equiv 0 \pmod m,$$

且 $$x^2+y^2+z^2+t^2\equiv 0 \pmod m.$$

由 $ay=bx$ 及 $ct\equiv dz \pmod m$ 推出第三个式子被 m 整除.

由 $az\equiv cx$ 及 $bt=dy \pmod m$ 推出第四个式子被 m 整除.

由 $at\equiv dx$ 及 $bz\equiv cy \pmod m$ 推出第五个式子被 m 整除.

利用问题 39 中的恒等式(改变 b,c,d 的符号)推出

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)\\&=(ax+by+cz+dt)^2+(ay-bx-ct+dz)^2\\&+(az+bt-cx-dy)^2+(at-bz+cy-dx)^2\end{aligned}$$

可被 m^2 整除.

若取 x,y,z,t 为绝对最小剩余,则 $x^2,y^2,z^2,t^2<\left(\frac{1}{2}m\right)^2$,因此

$$x^2+y^2+z^2+t^2=m'm<m^2.$$

将前面的等式除以 m^2,就将 $m'p$ 表示成了四平方之和.

51. 由问题 42 知,若 p 是奇素数,则 p 的一个比 p^2 小的倍数可以表示为四平方之和.若这个倍数比 p 大,那么根据问题 45(当倍数是偶数)或问题 50(当倍数是奇数)可知,有一个更小的 p 的倍数可以表示成四平方之和.

重复问题 45 或问题 50 的讨论若干次,就可推出 p 可以表为四平方之和.

这是使用 Fermat 递降法的一个例子.

52. 由素数 $2=1^2+1^2$ 及问题 51 知,每一个素数都可表示成四平方之和.根据问题 39,能表示成四平方之和的数集对乘法是封闭的,因此,所有正整数都可以表示成四平方之和.

53．只有 7 和 15 不能写成这种形式.

54．$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 1, 4^2 \equiv 0, 5^2 \equiv 1, 6^2 \equiv 4, 7^2 \equiv 1 \pmod 8$.

$$
\begin{array}{ccc}
 & +1 & +4 \\
\begin{array}{ccc} 0 & 1 & 4 \\ 1 & 2 & 5 \\ 4 & 5 & 0 \end{array} &
\begin{array}{ccc} 1 & 2 & 5 \\ 2 & 3 & 6 \\ 5 & 6 & 1 \end{array} &
\begin{array}{ccc} 4 & 5 & 0 \\ 5 & 6 & 1 \\ 0 & 1 & 4 \end{array}
\end{array}
$$

在这 27 种可能性中，7 没有在三平方和 (mod 8) 中出现.
$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 0, 3^2 \equiv 1 \pmod 4$.

$$
\begin{array}{cc}
 & +1 \\
\begin{array}{cc} 0 & 1 \\ 1 & 2 \end{array} &
\begin{array}{cc} 1 & 2 \\ 2 & 3 \end{array}
\end{array}
$$

这样，由 $x^2+y^2+z^2 \equiv 0 \pmod 4$ 推出 $x^2 \equiv y^2 \equiv z^2 \equiv 0 \pmod 4$.
若 $4m = x^2+y^2+z^2$，则 x, y, z 都是偶数，等式两边可以用 4 整除.

因此，若 $4^h(8k+7)$ 可以表示成三平方之和，则 $4^{h-1}(8k+7)$，$4^{h-2}(8k+7), \cdots, 8k+7$ 都可以表示成三平方之和. 但对 $8k+7$ 来说，这是不可能的，所以原假设不成立.

历 史 注 记

通过研究 Pythagoras 三元数组，Diophantus (约公元 200 年) 知道了如何把 $(a^2+b^2)(c^2+d^2)$ 表示为二平方之和. 1770 年，Euler 利用复数导出了同样的表达式. Diophantus 还知道二平方数之和不能同余于 3 (mod 4). Fermat 用他的递降法证明了，同余于 1 (mod 4) 的的素数可以表示成二平方之和，从而圆满地解决了二平方和问题. Fermat 还证明，素数的二平方和表示是唯一的 (问题 6.36).

Bachet (1621 年) 指出，Diophantus 假定每个数或是平方数，或是二平方之和，或是三平方之和，或是四平方之和. Fermat 第一个自称证明了这一假定. 1748 年，Euler 指出了如何将

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)$$

表示为四平方之和,并在 1751 年证明,每个素数是某个形如 $1+a^2+b^2$ 的数的因数.利用 Euler 的工作,在 1770 年,J.L.Lagrange 终于发表了一个完整的证明.四元数组是 W.R.Hamilton 在 1843 年提出的.

Fermat 判明了那些不能表示成三平方之和的数(问题 6.54),而在 1798 年,A.M.Legendre 证明,只有这些数不能表示成三平方之和.

第七章　分　　拆

Ferrers 图

1.　$1+1+1+1=2+1+1=2+2=3+1=4$.

因此，我们说正整数 4 有五种分拆[1].写出5 的七种分拆及 6 的十一种分拆．7 有多少种分拆？

2.　4 的五种分拆可以用这样的图来表示：

　　····　，　:··　，　∶∶　，　⋮˙　，　˙⋮　，

它们称为分拆图．给出 5 与 6 的分拆图．

3.　按列来看，图 :·· 给出了分拆 $2+1+1$．按行来看，这同一个图给出了分拆 $3+1$．变换行与列，就将图 :·· 变为 ⋮˙．称这样的一对分拆为共轭分拆．4 的哪一个分拆不与其他分拆共轭？对这样的分拆提出一个名称．找出不超过 10 的数的所有这样的分拆．

4.　写出不超过 10 的数的所有这样的分拆：它的部分数[2]是不相同的奇数．

5.　每个奇数至少有一个自共轭的分拆吗？

6.　设某数有一个自共轭分拆，它是否至少必有一个表为不同的奇数之和的分拆？

7.　若某个数的一个分拆的部分数是不相同的奇数，它是否必有一个自共轭分拆？

---

① 把一个正整数表为若干个正整数之和，称作这个正整数的一个分拆．在本章中，一个分拆的各项及其图形的各列（自左至右）均按大小顺序排列．—— 译者注．

② 把一个正整数表为若干个正整数之和，每一个被加数，称为这个分拆的部分数，例如 $2+1+1$ 是 4 的一个分拆，2,1,1 都是这个分拆的部分数．—— 译者注．

8. 猜测一个关于数 n 的自共轭分拆的个数与它的具有不同的奇部分数的分拆个数之间关系的定理，并证明之．

9. 写出 1,2,3,4,5,6,7 各数仅含 1 和 2 的分拆．

10. $2n$ 有多少个仅含 1 和 2 的分拆？

$2n+1$ 有多少个仅含 1 和 2 的分拆？

n 的仅含 1 和 2 的分拆的个数用 $p_2(n)$ 表示．

11. 写出 1,2,3,4,5,6,7 的仅有一个或两个部分数（可以相同）的所有分拆．

12. $2n$ 有多少个上题中所说的分拆？

$2n+1$ 有多少个这样的分拆？

13. 一个分拆的部分数如果只是 1 或 2，那么关于它的图能说些什么？

14. 如果一个分拆至多有两个部分数，那么关于它的图能说些什么？

15. 利用对图的讨论，在仅含数 1 和 2 的所有分拆的个数与至多含有两个部分数的所有分拆的个数之间建立联系．

生成函数

16. 计算

$$(1+x+x^2+\cdots+x^n+\cdots)(1+x^2+x^4+\cdots+x^{2n}+\cdots)$$

的展开式中的前八项．

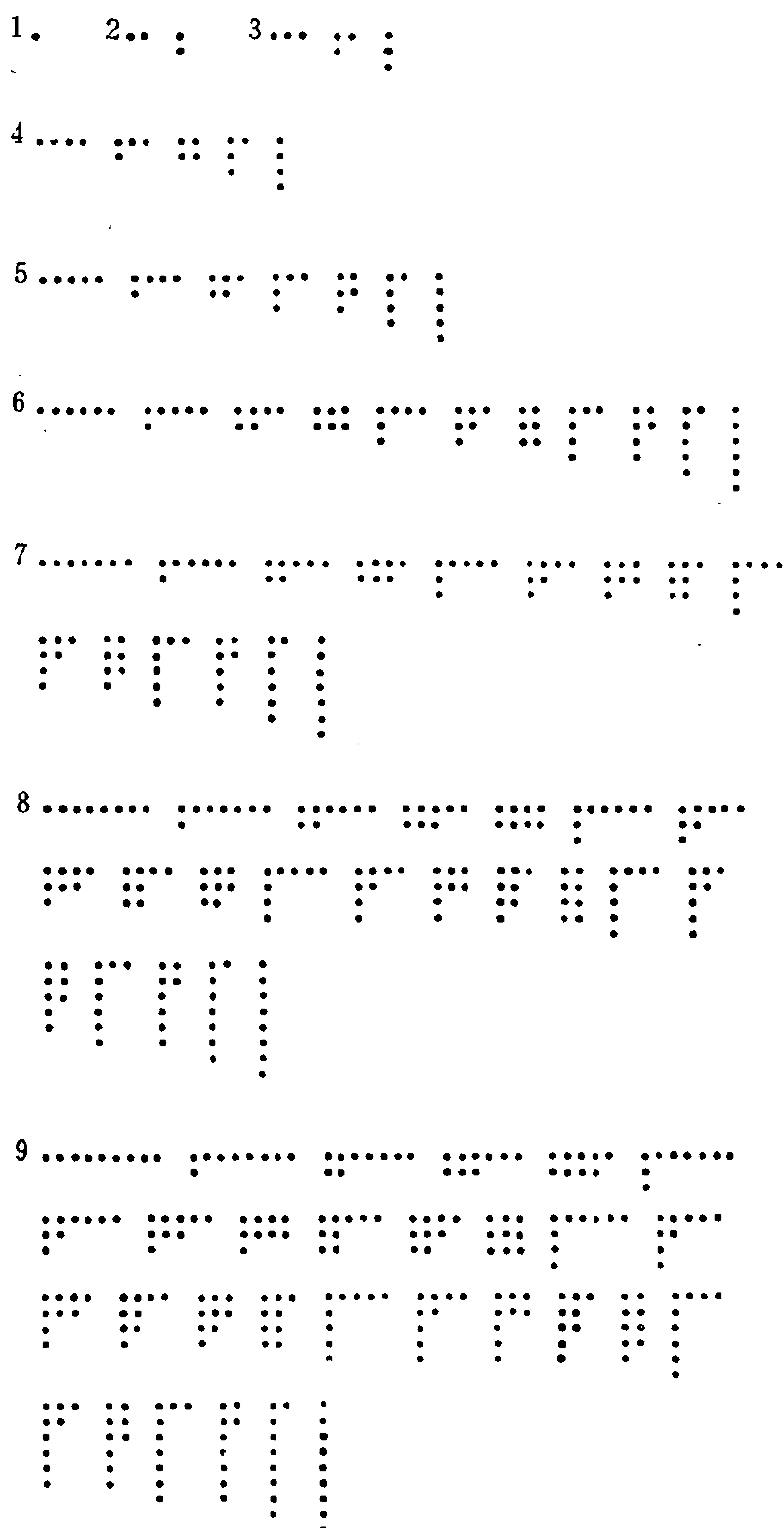
对这八项，把 x^n 的系数和 n 的仅含数 1 和 2 的分拆的个数做比较．

将第一个括号内的指数都写成若干个 1 的和，第二个括号内的指数都写成若干个 2 的和，一般地证明

$$(1+x+x^2+\cdots)(1+x^2+x^4+\cdots)=1+\sum_{n=1}^{\infty}p_2(n)x^n \quad ,$$

或者，利用当 $|x|<1$ 时的几何级数公式，证明

表 7.1 Ferrers 图



$$\frac{1}{(1-x)(1-x^2)} = 1+\sum_{n=1}^{\infty} p_2(n)x^n \quad .$$

$p_2(n)$的定义见问题 10 .

17. 算出 1,2,3,4,5,6,7,8,9 各数的仅含数 1,2或 3 的分拆的个数 . 这九个答案用$p_3(1)$, $p_3(2)$, $p_3(3)$,$p_3(4)$,$p_3(5)$, $p_3(6)$,$p_3(7)$,$p_3(8)$,$p_3(9)$表示 .

18. 算出 1 到 9 的每个整数的至多有三个部分数的分拆个数 .

19. 怎样描述部题 17 和问题 18 中的分拆图?

20. 计算

$$(1+x+x^2+\cdots+x^n+\cdots)(1+x^2+x^4+\cdots+x^{2n}+\cdots)\cdot$$
$$(1+x^3+x^6+\cdots+x^{3n}+\cdots)$$

的展开式的前七项. 对这七项 , 把$p_3(n)$与 x^n 的系数做比较 .

证明这个展开式中 x^n 的系数是$p_3(n)$, 而且当 $|x|<1$ 时 ,

$$\frac{1}{(1+x)(1-x^2)(1-x^3)} = 1+\sum_{n=1}^{\infty} p_3(n)x^n \quad .$$

21. 设 $|x|<1$, 对展开式

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)} = 1+\sum_{n=1}^{\infty} a_n x^n$$

中的系数 a_n 做一猜测 .

证实或否定你的猜测 .

通常将 a_n 写作 $p_4(n)$.

22. 用$p_m(n)$表示 n 的部分数 $\leqslant m$ 的分拆个数 . 仿照问题 16 ,问题 20 及问题 21 , 试猜测$p_m(n)$的生成函数.[1]

23. 设$p(n)$表示 n 的所有分拆的总数 ,在条件

(i) $m<n$,

(ii) $m=n$,

---

① 若 $F(x)=1+\sum_{n=0}^{\infty} a_n x^n$, 则称 $F(x)$是$\{a_n\}$的生成函数或母函数 . —— 译者注 .

(iii) $m>n$

之下，$p_m(n)$与$p(n)$有什么关系？

24. 给出一个无穷乘积，使它是$p(n)$的生成函数.

25. 对什么样的k值，$p_m(k)$等于n的这样的分拆的个数，它的最大部分数是m？

26. 对什么样的l值，$p_l(n)$等于n的这样的分拆的个数，它的部分数都小于m？

27. 利用问题25与问题26证明：当$n>m$时，

$$p_m(n)=p_m(n-m)+p_{m-1}(n).$$

若要使这个等式当$n=m$时成立，应规定$p_m(0)$取什么值？

若要使这个等式当$n<m$时成立，应规定$p_m(n-m)$取什么值？

28. 利用上题证明，若

$$F_m(x)=1+\sum_{n=1}^{\infty}p_m(n)x^n\ ,$$

则

$$F_m(x)=x^m F_m(x)+F_{m-1}(x)\ .$$

用归纳法证明你在问题22中提出的生成函数.

29. 设

$$\frac{1}{(1-x)(1-x^3)(1-x^5)\cdots(1-x^{2n-1})\cdots}=1+\sum_{n=1}^{\infty}q_n x^n\ ,$$

那么q_n等于n的哪种分拆的个数？

30. 设

$$\frac{1}{(1-x^2)(1-x^4)\cdots(1-x^{2n})\cdots}=1+\sum_{n=1}^{\infty}r_n x^n\ ,$$

那么r_n等于n的哪种分拆的个数？

31. 设

$$(1+x)(1+x^2)\cdots(1+x^n)\cdots=1+\sum_{n=1}^{\infty}s_n x^n\ ,$$

那么 s_n 等于 n 的哪种分拆的个数?

32. 设

$$(1+x)(1+x^3)\cdots(1+x^{2n-1})\cdots=1+\sum_{n=1}^{\infty}t_n x^n\ ,$$

那么 t_n 等于 n 的哪种分拆的个数?

33. 由恒等式

$$(1+x)(1+x^2)(1+x^3)\cdots(1+x^n)\cdots$$

$$=\frac{1-x^2}{1-x}\ \frac{1-x^4}{1-x^2}\ \frac{1-x^6}{1-x^3}\cdots\frac{1-x^{2n}}{1-x^n}\cdots$$

$$=\frac{1}{1-x}\ \frac{1}{1-x^3}\ \frac{1}{1-x^5}\cdots\frac{1}{1-x^{2n-1}}\cdots$$

能对 n 的分拆做何结论?

34. 设

$$(1+x+x^2)(1+x^2+x^4)(1+x^3+x^6)\cdots(1+x^n+x^{2n})\cdots$$

$$=1+\sum_{n=1}^{\infty}u_n x^n\ ,$$

那么 u_n 等于 n 的哪种分拆的个数?

35. 证明:n 的至多有两个部分数相等的分拆的个数,等于 n 的每个部分数不被 3 整除的分拆的个数.

Euler 定理

36. n 的有偶数个各不相同的部分数的分拆[1]个数用 $E(n)$ 表示,有奇数个各不相同的部分数的分拆[2]个数用 $O(n)$ 表示. 对于 $n=1,\cdots,9$, 求 $E(n)$ 与 $O(n)$. 对于哪些 $n\ (\leqslant 9)$, $E(n)=O(n)$?

---

[1] 这种分拆称为偶分拆. —— 译者注.

[2] 这种分拆称为奇分拆. —— 译者注.

37. 举出几个分拆图，每个分拆的各部分数都不同．

这些图有什么特点？

38. 对于你在问题 37 中举出的每个分拆图，若把它的最小部分数（设是 k）去掉，并在它的 k 个最大的部分数上每个加 1，试问是否会得到另一个各部分数都不相同的分拆？在什么情况下，这个变换不能实现？若这种变换可以实行，则称它为 α 变换．

39. 对于你在问题 37 中所举出的每个分拆图，若先把在通过最长一列的最后一个点的、从西南到东北方向的直线上的那些点都移去，再把这些点作为一个新的最短的列添加到原图上，试问这样是否构成另一个各部分数均不相同的分拆图？

在什么情况下，这个变换不能实现？

若这种变换可行，则称之为 β 变换．它对部分数的个数有何影响？

40. 除了问题 37 中的外，你再至少举出两个分拆图，它们的部分数都是各不相同的．对这每一个分拆图，以 k 表示其最短的列上的点数，以 l 表示上题所说的直线上的点的个数．

若 $k \leqslant l$，实行问题 38 中的变换 α（如果可能）；

若 $k > l$，实行问题 39 中的变换 β（如果可能）．

41. 在上题中，若 $k \leqslant l$ 但变换 α 不可行，证明 $k = l$，并求这个分拆中部分数的个数．证明这个分拆就是

$$(2l-1)+(2l-2)+\cdots+(l+1)+l=l^2+\frac{1}{2}(l-1)l$$

$$=\frac{1}{2}l(3l-1).$$

42. 在问题 40 中，若 $k > l$ 但变换 β 不可行，证明 $k = l+1$，并求这个分拆中部分数的个数．证明这个分拆就是

$$2l+(2l-1)+\cdots+(l+2)+(l+1)$$

$$=l^2+\frac{1}{2}l(l+1)=\frac{1}{2}l(3l+1).$$

43. 设$n\neq\frac{1}{2}l(3l\pm 1)$. 对于$n$的各部分数均不相同的分拆，定义如下的变换$T$：当$k\leqslant l$，$T=\alpha$；当$k>l$，$T=\beta$[1]. 证明：$T$是一一映射，并且将偶分拆变为奇分拆，而且反过来也对. 证明$E(n)=O(n)$.

44. 设$n=\frac{1}{2}l(3l\pm 1)$，证明：在n的具有不相同部分数的分拆中，唯一不能实行问题40中的变换的分拆有l个部分数. 对于每个n，求$E(n)-O(n)$之值.

45. 计算

$$(1-x)(1-x^2)(1-x^3)\cdots(1-x^n)\cdots$$

的展开式中的前九项.

46. 证明，当$|x|<1$时，

$$(1-x)(1-x^2)(1-x^3)\cdots(1-x^n)\cdots=1+\sum_{n=1}^{\infty}(E(n)-O(n))x^n.$$

47. 证明，当$|x|<1$时，

$$(1-x)(1-x^2)(1-x^3)\cdots(1-x^n)\cdots=\sum_{n=-\infty}^{\infty}(-1)^n x^{\frac{1}{2}n(3n-1)}.$$

(Euler 定理).

注记与答案

本章是作为一个插曲，它与前面几章的定理无关，也与后面的各章内容无关. 参考书见书目: Andrews (1971), Chrystal (1964).

1. 2+1+1与1+2+1，1+1+2被看作是4的同一个分拆. 我们仅研究这些部分数本身，而不计较它们在和式中的次序.

---

[1] k，l的意义同40题. —— 译者注.

$$1+1+1+1+1=2+1+1+1=2+2+1$$
$$=3+1+1=3+2=4+1=5.$$
$$1+1+1+1+1+1=2+1+1+1+1$$
$$=2+2+1+1=2+2+2$$
$$=3+1+1+1=3+2+1=3+3$$
$$=4+1+1=4+2=5+1=6.$$

7有15个分拆.

n的分拆个数用$p(n)$表示，$p(4)=5$，$p(5)=7$，$p(6)=11$，$p(7)=15$.

2. 许多书中是把这些点列竖排而不是横排，于是图……表示5的只有一个部分数的分拆，而不是像我们这里所表示的是五个部分数.

5 ……, :…, ::·, ⋮··, ::·, ⋮:, ⋮

6 ……, :…, ::··, :::, ⋮…, ⋮:·,

:::, ⋮··, ⋮:, ⋮·, ⋮

这些图通常称为Ferrers图，以区别于那些有边和内部区域的图.

3. ::是自共轭的.

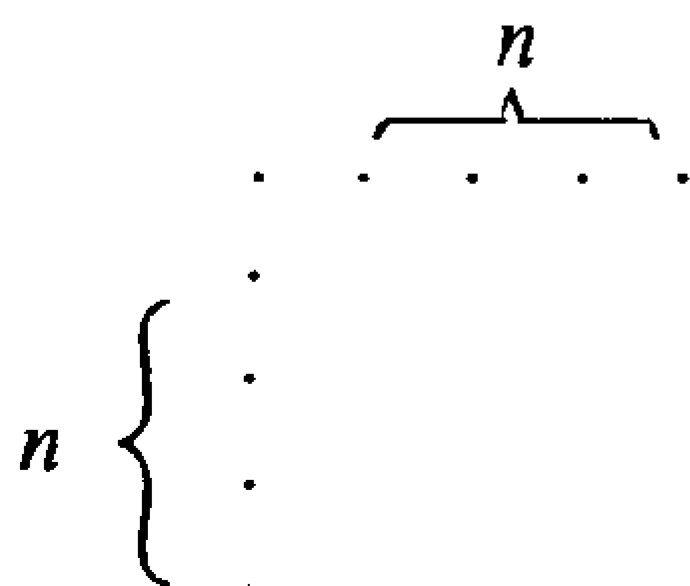
1 ·, 2 无, 3 :·, 4 ::, 5 ⋮··,

6 ⋮:·, 7 ⋮···, 8 :::, ⋮:··,

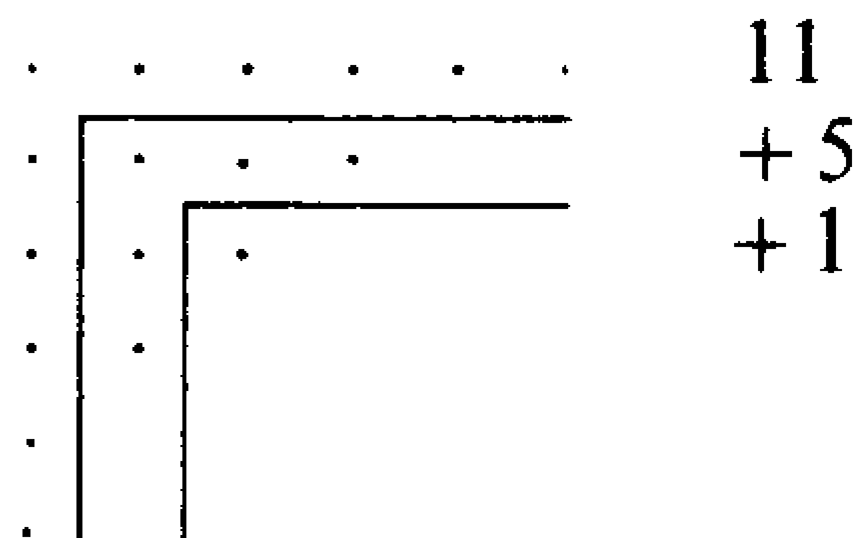
9 :::, ⋮····, 10 ⋮::·, ⋮:···

4. $1=1$，$3=3$，$4=3+1$，$5=5$，$6=5+1$，$7=7$，$8=5+3=7+1$，$9=5+3+1=9$，$10=7+3=9+1$.

5. $2n+1$ 可以分拆成 $(n+1)+\underbrace{1+\cdots+1}_{n个}$，它的图是



6. 是，例如



7. 分拆中的每个奇数有问题 5 中的 L 型点列图. 若这些奇数互不相同，就可以按大小将这些 L 型点列像问题 6 那样地放在一起，从而构成这个分拆的图.

因为每一个 L 型点列是自共轭的，所以得到的是一个自共轭图.

9. $1=1$

$2=2=1+1$

$3=2+1=1+1+1$

$4=2+2=2+1+1=1+1+1+1$

$5=2+2+1=2+1+1+1=1+1+1+1+1$

$6=2+2+2=2+2+1+1=2+1+1+1+1$

$\quad=1+1+1+1+1+1$

$7=2+2+2+1=2+2+1+1+1=2+1+1+1+1+1$

$\quad=1+1+1+1+1+1+1$

10. $2n=n$个$2=(n-1)$个$2+2$个$1=(n-k)$个$2+2k$个1，$k\leqslant n$. 因此，恰好有 $n+1$ 个这种形式的分拆. $2n+1=(2n)+1$，

所以 $2n+1$ 也恰好有 $n+1$ 个这样的分析．

$$p_2(n)=\left[\frac{1}{2}n\right]+1 \quad .$$

11． $1, 2=1+1, 3=2+1, 4=3+1=2+2, 5=4+1=3+2$，$6=5+1=4+2=3+3, 7=6+1=5+2=4+3$．

12． $n+1$，$n+1$．

13． 至多二行．

14． 至多二列．

15． 这两种类型出现在共轭对中，因此，n 的部分数 $\leqslant 2$ 的分拆的个数 $p_2(n)$ 等于 n 的至多含两个部分数的分拆的个数．

16． $1+x+2x^2+2x^3+3x^4+3x^5+4x^6+4x^7+\cdots$

n 的每一个仅含 1 或 2 的分拆，使乘积中的 x^n 的系数增加 1．

若 $n=\underbrace{2+2+\cdots+2}_{a\text{个}}+\underbrace{1+1+\cdots+1}_{b\text{个}}$，则 $x^n=x^b x^{2a}$．

$\dfrac{1}{(1-x)(1-x^2)}$ 称为 $p_2(n)$ 的生成函数．

17． $p_3(1)=1$，$p_3(2)=2$，$p_3(3)=3$，$p_4(4)=4$，$p_3(5)=5$，$p_3(6)=7$，$p_3(7)=8$，$p_3(8)=10$，$p_3(9)=12$．

18． 与问题 17 的答案相同．

19． 问题 17 中的图至多有三行．

问题 18 中的图至多有三列．

这两种类型的分拆都是成对共轭的．

20． $1+x+2x^2+3x^3+4x^4+5x^5+7x^6+8x^7+10x^8+12x^9+\cdots$

若 $n=\underbrace{3+3+\cdots+3}_{a\text{个}}+\underbrace{2+2+\cdots+2}_{b\text{个}}+\underbrace{1+1+\cdots+1}_{c\text{个}}$，

则 $x^n=x^c x^{2b} x^{3a}$．因此，这个分拆使乘积中的 x^n 的系数增加 1．x^n 的系数中的每一个单位，都是以这种方式从一个这种类型的分拆得到的．

当 $|x|<1$， $1+x+x^2+\cdots=\dfrac{1}{1-x}$，

$$1+x^2+x^4+\cdots=\frac{1}{1-x^2}，$$

$$1+x^3+x^6+\cdots=\frac{1}{1-x^3}.$$

$\dfrac{1}{(1-x)(1-x^2)(1-x^3)}$ 是$p_3(n)$的生成函数．

21. 左端是

$$(1+x+x^2+\cdots)(1+x^2+x^4+\cdots)$$
$$(1+x^3+x^6+\cdots)(1+x^4+x^8+\cdots)，$$

所以，乘积中的每个 x^n 产生自 n 的一个各部分数 $\leqslant 4$ 的分拆，因此，系数 a_n 就是这种分拆的个数．

22. $\dfrac{1}{(1-x)(1-x^2)(1-x^3)\cdots(1-x^m)}$．这是问题 21 的一个明显的推广，其证明见问题 28．

23. 当 $m<n$ 时，$p(n)>p_m(n)$．

当 $m\geqslant n$ 时，$p(n)=p_m(n)$.

24. $\dfrac{1}{(1-x)(1-x^2)\cdots(1-x^m)\cdots}$．

25. $k=n-m$．

26. $l=m-1$．

27. $p_m(n)=n$ 的各部分数 $\leqslant m$ 的分拆的个数

$=n$ 的最大部分数是 m 的分拆的个数 $+n$ 的各部分数 $\leqslant m-1$ 的分拆的个数

$=p_m(n-m)+p_{m-1}(n)$．

当 $m=n$ 时，n 恰好有一个分拆，其最大部分数是 m；故取 $p_m(0)=1$．

当 $m>n$ 时，因为 $p_m(n)=p_{m-1}(n)$，故取 $p_n(n-m)=0$.

28. $$F_m(x)=1+\sum_{n=1}^{\infty}p_m(n)x^n$$

$$=1+\sum_{n=1}^{\infty}(p_m(n-m)+p_{m-1}(n))x^n$$

$$=1+\sum_{n=1}^{\infty}p_{m-1}(n)x^n+\sum_{n=1}^{\infty}p_m(n-m)x^{n-m}x^m.$$

当 $n\leqslant m$ 时，$p_m(n-m)$ 取问题 27 中所给出的值，得到

$$F_m(n)=F_{m-1}(x)+\left[1+\sum_{n-m=1}^{\infty}p_m(n-m)x^{n-m}\right]x^m$$

$$=F_{m-1}(x)+x^mF_m(x).$$

29. q_n 是 n 的部分数全是奇数的分拆个数.

30. r_n 是 n 的部分数全是偶数的分拆个数.

31. s_n 是 n 的部分数互不相同的分拆个数.

32. t_n 是 n 的部分数是互不相同的奇数的分拆个数.

33. n 的部分数互不相同的分拆的个数等于 n 的部分数都是奇数的分拆的个数.

34. 这个乘积中的每一个元素是由在每个括号中各取一项(即从 $1+x^n+x^{2n}$ 中取出 x^0，或 x^n，或 x^{n+n})相乘而得到的，因此，相应的分拆中的部分数至多有两个相同.

35. $(1+x+x^2)(1+x^2+x^4)\cdots(1+x^n+x^{2n})\cdots$

$$=\frac{1-x^3}{1-x}\ \frac{1-x^6}{1-x^2}\cdots\frac{1-x^{3n}}{1-x^n}\cdots$$

$$=\frac{1}{(1-x)(1-x^2)(1-x^4)(1-x^5)\cdots(1-x^{3n-2})(1-x^{3n-1})\cdots}.$$

36. $E(1)=0$ $O(1)=1$ $E(n)-O(n)=-1$

$E(1)=0$	$O(1)=1$	-1
$E(2)=0$	$O(2)=1$	-1
$E(3)=1$	$O(3)=1$	0
$E(4)=1$	$O(4)=1$	0
$E(5)=2$	$O(5)=1$	1
$E(6)=2$	$O(6)=2$	0
$E(7)=3$	$O(7)=2$	1
$E(8)=3$	$O(8)=3$	0
$E(9)=4$	$O(9)=4$	0

37. 连结相邻两列的最后一个点的直线的斜率 $\geqslant 1$.

38.

可行 α

不可行

可行 α

当部分数的个数大于最小部分数时，变换 α 可行.

经变换 α 后，减少了一个部分数，所以改变了分拆的奇偶性.

39.

可行 β

不可行

当所说的斜线上的点数小于最短列上的点数，且在该斜线上没有最短列上的点时，变换 β 是可行的．变换 β 使部分数增加了一个，所以改变了分拆的奇偶性．

40.

· · ·
· ·
· ·
·

$k<l$，α 总是可行的．

· · ·
· · ·
· ·
· ·
·

$k=l$，α 有时是可行的．

· ·
· ·
·

$k=l$，当斜线与最短列相交时，α 不可行．

· · · ·
· · · ·
· · · ·
· · · ·
· · · ·
· · ·
· · ·
· ·
·

$k>l+1$，β 总是可行的．

· · ·
· · ·
· · ·
· ·
· ·
·

$k=l+1$，β 有时是可行的．

· · ·
· · ·
· · ·
· · ·
· ·
·

$k=l+1$，当斜线与最短列相交时，β 不可行．

41，42．见上面所说明的各种情况．

43．设 P 是 n 的一个分拆，它的部分数各不相同，最小部分数为 k，它的 Ferrers 图中的最低的东北方向斜线[1]上有 l 个点．因为 $n\neq\frac{1}{2}l(3l\pm1)$（$l$ 是任意整数），我们可以定义变换 $T:P\to P'$．若对于 P 有 $k\leqslant l$，则对于 P' 有 $k>l$；反之亦然．映射 α 减少一个部分数，而映射 β 则增加一个部分数．若变换 T 使 $P\to P'$ 及 $Q\to P'$，那么，或者对于 P 和 Q 都有 $k\leqslant l$，或者对于 P 和 Q 都有 $k>l$，因此，或者在两种情况下都是 $T=\alpha$，或者在两种情况下都是 $T=\beta$，所以 P 和 Q 的部分数的个数相同．若对于 P 和 Q 都是 $k\leqslant l$，则（P' 的 l）=（P 的 k）=（Q 的 k），因此 P 和 Q 有相同的最小部分数．由于只是最短的列被 T 移动，所以 $P=Q$．若对于 P 和 Q 都是 $k>l$，则（P' 的 k）=（P 的 l）=（Q 的 l）．因为只有斜线上的 l 个点被 T 移动，所以仍是 $P=Q$．故而 T 是一一映射，且将具有偶数个各不相同的部分数的分拆映到具有奇数个各不相同的部分数的分拆；反过来也对．因此，$E(n)=O(n)$．

44．由问题 41 和问题 42 见到，在变换 α 或 β 不可实行的情形，分拆都是有 l 个部分数．$(-1)^l=1$（l 是偶数）或 -1（l 是奇数），因此 $E(n)-O(n)=0\left(当\ n\neq\frac{1}{2}l(3l\pm1)\right)$ 以及 $E(n)-O(n)=(-1)^l\left(当\ n=\frac{1}{2}l(3l\pm1)\right)$．

45．$1-x-x^2+x^5+x^7+\cdots$

46．乘积中各项的绝对值是由各部分数都不相同的那些分拆形成的，对应着奇数个部分数的分拆的项是负号，对应着偶数个部分数的分拆的项是正号．

---

[1] 见问题 39.—— 译者注．

47. $(1-x)(1-x^2)\cdots(1-x^n)\cdots$

$$=1+\sum_{n=1}^{\infty}(E(n)-O(n))x^n$$

$$=1+\sum_{l=1}^{\infty}(-1)^l x^{\frac{1}{2}l(3l-1)}+\sum_{l=1}^{\infty}(-1)^l x^{\frac{1}{2}l(3l+1)}$$

$$=1+\sum_{l=1}^{\infty}(-1)^l x^{\frac{1}{2}l(3l-1)}+\sum_{l=-1}^{-\infty}(-1)^l x^{\frac{1}{2}(-l)(-3l+1)}$$

$$=1+\sum_{l=1}^{\infty}(-1)^l x^{\frac{1}{2}l(3l-1)}+\sum_{l=-1}^{-\infty}(-1)^l x^{\frac{1}{2}l(3l-1)}$$

$$=\sum_{l=-\infty}^{\infty}(-1)^l x^{\frac{1}{2}l(3l-1)}.$$

历 史 注 记

分拆理论首先是由 L. Euler 在十八世纪四十年代发展起来的．分拆图是由 N. M. Ferrers 提出的，并于 1853 年在 J. J. Sylvester 的一篇文章中第一次出现．我们所用的 Euler 定理的证明 (问题 7.36 — 7.47)属于 F. Franklin (1881)．在 Dickson 的书 (1950)的第二卷第三章中，全面地介绍了这一课题的历史．

第八章 二 次 型

幺模变换

首先，我们考察正方形格到自身的变换.

1. 在一张方格纸上，选四个格点 A, B, C, D, 使得以它们为顶点的平行四边形 Π 的内部及其边界上除顶点外没有其他格点. 设 τ 是将 A 映射到 B 的格平移[1]. 画出 Π 经平移 τ 后的像的草图. 设 σ 是将 A 映射到 D 的格平移. 画出 Π 经平移 σ 后的像的草图. 在 $\tau(\Pi)$ 和 $\sigma(\Pi)$ 的内部及边界上有无格点？对于任何整数 m, n, $\tau^m(\Pi)$ 或 $\sigma^n(\Pi)$[2] 的内部或边界上有无格点？

2. 用上题记号. 平面上的每个点是否总在一个或几个平行四边形 $\tau^m\sigma^n(\Pi)$ 的内部或边界上？每个格点是否必是四个这样的平行四边形的顶点？

3. 利用通常的笛卡尔平面直角坐标系，全体方格点可以用全体有序整数对来一一标记. 设 $ABCD$ 是问题 1 中的格点平行四边形，我们可取 A 做为坐标系的原点. 设 $B=(a, b)$, $D=(c, d)$, C 是与 A 相对的顶点，那么 C 的坐标是什么？在线性变换 α: $(x, y)\to(x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 之下，单位正方形 $\{(0, 0), (1, 0), (1, 1), (0, 1)\}$ 的像是什么？在变换 α 之下，形如 $(x, 0)$ 的格点的像是什么？形如 $(0, y)$ 的格点的像是什么？设 k, l 是任意整数，则与

---

① 关于格变换，见第九章问题 7. —— 译者注.

② $\tau^m(\Pi)=\tau(\tau^{m-1}(\Pi))$, $\sigma^n(\Pi)=\sigma(\sigma^{n-1}(\Pi))$. —— 译者注

坐标轴平行的两族直线 $x=k$ 与 $y=l$ 构成一个由单位正方形组成的格子．这个格子在线性变换 α 之下的像是什么？

4．问题 3 中的线性变换 α 是否将格点集合满射到自身？

5．设 $A=(0,0)$，$B=(a,b)$，$C=(a+c,b+d)$ 且 $D=(c,d)$，求平行四边形 $ABCD$ 的面积．

若 $ad-bc=0$，那么点 A,B,C,D 有何关系？

6．设在线性变换

$$\alpha:(x,y)\to(x,y)\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

之下，点 (r,s) 及 (t,u) 的像相同，证明

$$\alpha:(r-t,s-u)\to(0,0).$$ [1]

设对于 $y\neq 0$，$\alpha:(0,y)\to(0,0)$，证明 $c=d=0$．

设对于 $x\neq 0$，$\alpha:(x,y)\to(0,0)$，证明 $ad-bc=0$．

证明：若变换 α 不是一一对应的，则 $ad-bc=0$．

7．设平行四边形 $ABCD$ 的四个顶点不共线，证明问题3中的 α 是 $\mathbf{Z}^2$ [2] 到 $\mathbf{Z}^2$ 的双射．

8．使用问题 3 中的记号，$ad-bc$ 是否必是整数？

求被 α 映射到 $(1,0)$ 的点．

求被 α 映射到 $(0,1)$ 的点．

$$\frac{a}{ad-bc},\ \frac{b}{ad-bc},\ \frac{c}{ad-bc},\ \frac{d}{ad-bc}$$

是否都是整数？

证明 $\dfrac{a}{ad-bc}\,\dfrac{d}{ad-bc}-\dfrac{b}{ad-bc}\,\dfrac{c}{ad-bc}$

是整数，并推出 $ad-bc=\pm 1$．

9．设 a,b,c,d，是整数且 $ad-bc=\pm 1$，变换

---

① “$\alpha:(x,y)\to(u,v)$”表示：变换 α 将 (x,y) 映射为 (u,v)．——译者注．

② $\mathbf{Z}^2$ 表示平面上的两个坐标都是整数的点所成的集合．——译者注．

$$(x,y)\to(x,y)\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

是否必将 $\mathbf{Z}^2$ 满射到 $\mathbf{Z}^2$？

10. 一个以格点为顶点且在其内部和边界上无另外格点的平行四边形的面积等于多少?

11. 设 M 是三角形 ABC 的边 BC 的中点，A' 是 A 在关于 M 做半周旋转后的像．$ABA'C$ 是怎样的四边形？若 A，B，C 是一个无限方格中的格点，那么 A' 是否也是这个方格中的格点？若在三角形 ABC 的内部，或在它的边界上（除顶点外）没有格点，那么对 $ABA'C$ 是否能有同样的结论？

12. 设 A，B，C 是一个无限方格中的格点，而且在三角形 ABC 的内部及边界上无其他格点，求它的面积．

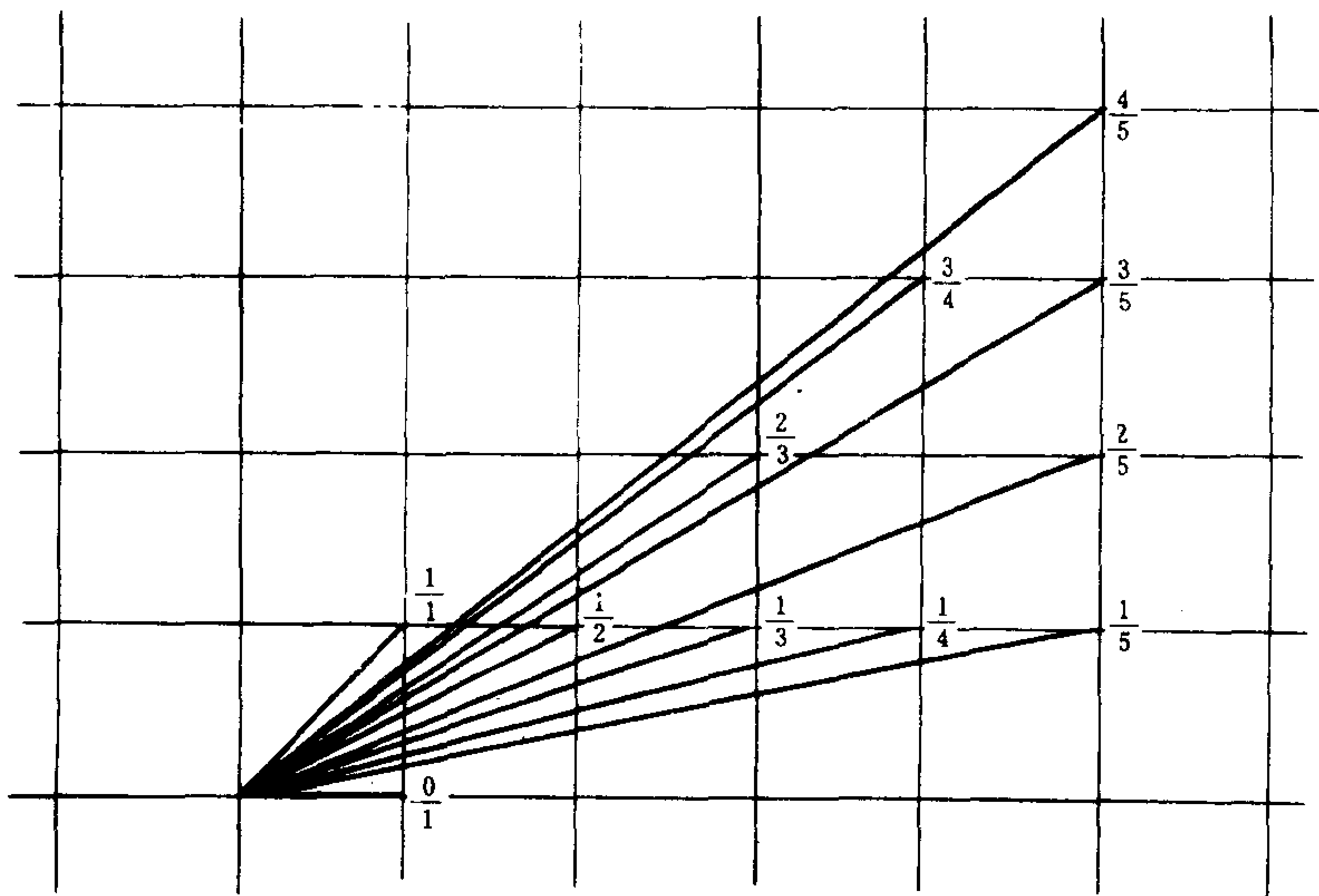


图 8.1

13. 在以 (0，0)，(5，0) 及 (5，5) 为顶点的三角形中，画出以原点到这个三角形内部和边界上的各个格点的线段．这些线段的斜率（以严格的递增顺序列出）是

$$0, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, 1.$$

这样排列的十一个数所组成的集合，称为 Farey 数列 F_5. 写出 Farey 数列 F_6，即由介于 0 与 1 之间按递增顺序排列的有理数 $\frac{p}{q}$ 所组成的集合，其中 $0 \leqslant p \leqslant q \leqslant 6$, $\gcd(p, q) = 1$.

14. 设 a, b, c, d, e, f 是正整数，$\frac{a}{b}$，$\frac{c}{d}$，$\frac{e}{f}$ 是某个 Farey 数列中的相邻项. 通过考虑以 $(0,0)$, (b,a), (d,c) 为顶点的三角形，证明 $ad - bc = -1$.

推导 $cf - de = -1$ 及 $\frac{c}{d} = \frac{a+e}{b+f}$.

15. 设 p, q, r, s 是整数，当 $ps - qr = \pm 1$ 时，称变换

$$(x, y) \to (x, y)\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

为幺模变换，称矩阵 $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ 为幺模矩阵.

在幺模变换下，单位正方形的像的面积多大？

16. 幺模矩阵的转置矩阵是幺模矩阵吗？它的逆矩阵呢？

17. 证明：幺模矩阵的集合对于矩阵乘法构成一个群.

由幺模变换构成的相应的群称为幺模群. 为了方便，有时把这个群看作是作用于方格，有时则看作是作用于全平面.

18. 设 $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ 是幺模矩阵，$X = px + ry$, $Y = qx + sy$，说明为什么 $\gcd(x, y) \mid X, Y$. 证明：$x = \pm(sX - rY)$, $y = \pm(-qX + pY)$, $\gcd(x, y) = \gcd(X, Y)$.

19. 矩阵

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

都是幺模矩阵，说明每个相应的幺模变换的几何意义.

20. 找出幺模群的一个指数为 2 的子群.

由所有形如 $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ 的矩阵所组成的幺模群的子集是否构成一个子群？

等价二次型

21. 小于 10 的数中，哪些可以写成 x^2+y^2 的形式，其中 x，y 都是整数？

在方格纸上画出在其上有格点的圆 $x^2+y^2=n$，其中 $n<10$. 这些圆与哪些值 n 对应？

22. 设 x，y 只取整数值，表达式

$$(x+y)^2+y^2=x^2+2xy+2y^2$$

能取哪些比 10 小的值？

它们是否都是正值？

3 是可能取到的值吗？

23. 设 x，y 只取整数值，二次型

$$(x+2y)^2+y^2=x^2+4xy+5y^2$$

能取哪些比 10 小的值？

对于给定的整数 m，n，能否选取整数 x，y，使得

$$x+2y=m,\ y=n\quad ?$$

24. 利用问题 9，说出 p，q，r，s 所应满足的条件，使得二次型

$$(px+ry)^2+(qx+sy)^2 \quad 与 \quad x^2+y^2$$

取完全相同的整数值集合.

25. 因为变换

$$(x,y)\to(x+y,y)$$

把整数 $\mathbf{Z}^2$ 满射到自身，所以二次型 x^2+y^2 与 $(x+y)^2+y^2$ 所取的整数值集合完全相同. 我们称它们为等价的二次型.[1]

证明点 $(a+b,b)$ 在圆 $x^2+y^2=25$ 上的充要条件是 (a,b) 在曲线 $(x+y)^2+y^2=25$ 上.

这样，变换 $(x,y)\to(x+y,y)=(x,y)\begin{pmatrix}1&0\\1&1\end{pmatrix}$ 就把曲线

---

1 关于等价二次型的定义，见对本题的注记. —— 译者注.

$(x+y)^2+y^2=25$ 满射到圆 $x^2+y^2=25$. 说明变换 $(x,y)\rightarrow(x,y)\begin{pmatrix}1&0\\1&1\end{pmatrix}$的几何意义. 利用这个变换来检验图 8.2 中所画的椭圆 $x^2+2xy+2y^2=25$ 的精确程度.

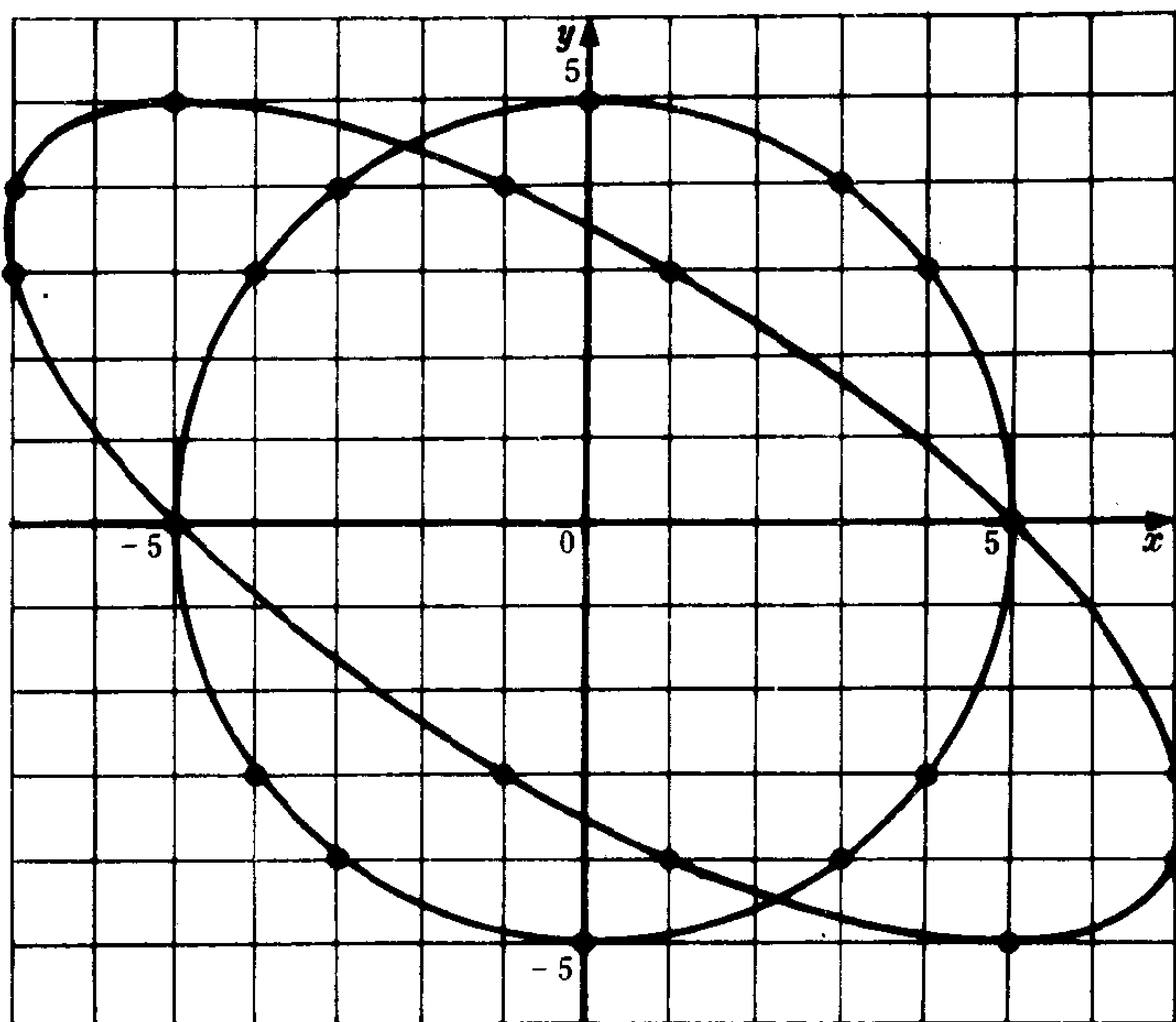


图 8.2

26. 变换 $(x,y)\rightarrow(x+y,y)$将三个椭圆

$$x^2+2xy+2y^2=9,$$

$$x^2+2xy+2y^2=16,$$

以及

$$x^2+2xy+2y^2=25$$

映射成什么曲线?

画出这三个椭圆的草图.

27. 表 8.1 中列出了当 x,y 取 -5 与 5 之间的整数值时,二

次型

$$x^2-2xy+3y^2\ ,$$
$$x^2+2y^2\ ,$$
$$x^2+2xy+3y^2\ ,$$
$$x^2+4xy+6y^2$$

所取的数值．证明这四个二次型是等价的．

表 8.1

$x^2-2xy+3y^2$

$y=+5$	150	131	114	99	86	75	66	59	54	51	50
$+4$	113	96	81	68	57	48	41	36	33	32	33
$+3$	82	67	54	43	34	27	22	19	18	19	22
$+2$	57	44	33	24	17	12	9	8	9	12	17
$+1$	38	27	18	11	6	3	2	3	6	11	18
0	25	16	9	4	1	0	1	4	9	16	25
-1	18	11	6	3	2	3	6	11	18	27	38
-2	17	12	9	8	9	12	17	24	33	44	57
-3	22	19	18	19	22	27	34	43	54	67	82
-4	33	32	33	36	41	48	57	68	81	96	113
-5	50	51	54	59	66	75	86	99	114	131	150
$x=$	-5	-4	-3	-2	-1	0	1	2	3	4	5

x^2+2y^2

$y=+5$	75	66	59	54	51	50	51	54	59	66	75
$+4$	57	48	41	36	33	32	33	36	41	48	57
$+3$	43	34	27	22	19	18	19	22	27	34	43
$+2$	33	24	17	12	9	8	9	12	17	24	33
$+1$	27	18	11	6	3	2	3	6	11	18	27
0	25	16	9	4	1	0	1	4	9	16	25
-1	27	18	11	6	3	2	3	6	11	18	27
-2	33	24	17	12	9	8	9	12	17	24	33
-3	43	34	27	22	19	18	19	22	27	34	43
-4	57	48	41	36	33	32	33	36	41	48	57
-5	75	66	59	54	51	50	51	54	59	66	75
$x=$	-5	-4	-3	-2	-1	0	1	2	3	4	5

$$x^2+2xy+3y^2$$

y= +5	50	51	54	59	66	75	86	99	114	131	150
+4	33	32	33	36	41	48	57	68	81	96	113
+3	22	19	18	19	22	27	34	43	54	67	82
+2	17	12	9	8	9	12	17	24	33	44	57
+1	18	11	6	3	2	3	6	11	18	27	38
0	25	16	9	4	1	0	1	4	9	16	25
−1	38	27	18	11	6	3	2	3	6	11	18
−2	57	44	33	24	17	12	9	8	9	12	17
−3	82	67	54	43	34	27	22	19	18	19	22
−4	113	96	81	68	57	48	41	36	33	32	33
−5	150	131	114	99	86	75	66	59	54	51	50
x=	−5	−4	−3	−2	−1	0	1	2	3	4	5

$$x^2+4xy+6y^2$$

y= +5	75	86	99	114	131	150	171	194	219	246	275
+4	41	48	57	68	81	96	113	132	153	176	201
+3	19	22	27	34	43	54	67	82	99	118	139
+2	9	8	9	12	17	24	33	44	57	72	89
+1	11	6	3	2	3	6	11	18	27	38	51
0	25	16	9	4	1	0	1	4	9	16	25
−1	51	38	27	18	11	6	3	2	3	6	11
−2	89	72	57	44	33	24	17	12	9	8	9
−3	139	118	99	82	67	54	43	34	27	22	19
−4	201	176	153	132	113	96	81	68	57	48	41
−5	275	246	219	194	171	150	131	114	99	86	75
x=	−5	−4	−3	−2	−1	0	1	2	3	4	5

28．若将变换

$$(x,y)\to(x,y)\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

写成列向量形式

$$\begin{pmatrix}x\\y\end{pmatrix}\to\begin{pmatrix}p&q\\r&s\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix},$$

那么p，q，r，s应该取什么值？

29．$x^2+2y^2=(x\quad y)\begin{pmatrix}1&0\\1&2\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$.

$$x^2+2xy+3y^2=(x\quad y)\begin{pmatrix}1&1\\1&3\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}.$$

计算矩阵乘积

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

并证明 $(a,\ b)$ 在曲线 $x^2+2xy+3y^2=k$ 上的充要条件是 $(a\ ,b)\begin{pmatrix}1&0\\1&1\end{pmatrix}$ 在曲线 $x^2+2y^2=k$ 上.

30. 由问题 24 知道，当 $p\ ,q\ ,r\ ,s$ 是整数且 $ps-qr=\pm 1$ 时，x^2+2y^2 与 $(px+ry)^2+2\ (qx+sy)^2$ 是等价的二次型. 求矩阵 P，使得

$$(px+ry)^2+2(qx+sy)^2=(x\quad y)\,P\begin{pmatrix}1&0\\0&2\end{pmatrix}P^{\mathrm{T}}\begin{pmatrix}x\\y\end{pmatrix},$$

其中 P^{T} 表示 P 的转置矩阵.

31. 当 $(x\ ,y)\rightarrow(px+ry\ ,\ qx+sy)$ 是幺模变换时，

$$ax^2+bxy+cy^2=(x\quad y)\begin{pmatrix}a&\frac{1}{2}b\\\frac{1}{2}b&c\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

与

$$a\ (px+ry)^2+b\ (px+ry)(qx+sy)+c\ (qx+sy)^2$$

是等价的二次型.

求矩阵 P，使得

$$a\ (px+ry)^2+b\ (px+ry)(qx+sy)+c\ (qx+sy)^2$$
$$=(x\quad y)P\begin{pmatrix}a&\frac{1}{2}b\\\frac{1}{2}b&c\end{pmatrix}P^{\mathrm{T}}\begin{pmatrix}x\\y\end{pmatrix}.$$

判　别　式

我们要找一个容易判别的、等价二次型所共有的性质.

32. 适当选取相应的对称矩阵 M，将二次型

$$x^2-2xy+3y^2\ ,$$
$$x^2+2y^2\ ,$$
$$x^2+2xy+3y^2\ ,$$

$$x^2+4xy+6y^2$$

写成$(x\quad y)M\begin{pmatrix}x\\y\end{pmatrix}$的形式.

计算这四个矩阵的行列式.

33. 利用问题 17 证明,两个 2×2 矩阵之积的行列式等于这两个矩阵的行列式之积.

设 P 是幺模矩阵且 $A=\begin{pmatrix}a & b\\c & d\end{pmatrix}$,证明 PAP^{T} 的行列式是$ad-bc$.

34. 设 A,B 都是对称矩阵,且使得$(x\quad y)A\begin{pmatrix}x\\y\end{pmatrix}$与$(x\quad y)B\begin{pmatrix}x\\y\end{pmatrix}$是等价的二次型,证明 A 与 B 的行列式相等.

35. 设 $ax^2+bxy+cy^2$ 与 $a'x^2+b'xy+c'y^2$ 是等价的二次型,利用上题推出 a,b,c,a',b',c'之间的关系.

36. 对于二次型 x^2+y^2, x^2 与 x^2-y^2, 求 b^2-4ac 之值. 画出 $x^2+y^2=1$,$x^2=1$ 及 $x^2-y^2=1$ 的草图.

37.
$$\begin{aligned}4a\,(ax^2+bxy+cy^2)&=4a^2x^2+4abxy+4acy^2\\&=(2ax+by)^2+(4ac-b^2)y^2.\end{aligned}$$

数值 b^2-4ac 称为二次型 $ax^2+bxy+cy^2$ 的判别式.

利用问题 34,证明等价二次型的判别式相同.

当 $b^2-4ac<0$ 时,考察上面等式右端所可能取的值,并证明在这种情形下,$ax^2+bxy+cy^2$ 必与 a 同号.

38. 当 $b^2-4ac<0$ 时,称二次型 $ax^2+bxy+cy^2$ 是定二次型.若还有 $a>0$,则称为正定二次型;若还有 $a<0$,则称为负定二次型.

设 $ax^2+bxy+cy^2$ 是正定的,$a'x^2+b'xy+c'y^2$ 是与它等价的二次型,证明 $a'x^2+b'xy+c'y^2$ 也是正定的.

39. 举一个不是定二次型的例子,并且指出,它若不是既取正值又取负值,就必然对于无限多对(x,y)取零值.

40. 设 a,b,c是整数,b^2-4ac能不能等于 -1 或 -2?考虑对于模 4 的各种可能性,并将你的结论推广到以下情形:

(i) b是偶数, (ii) b是奇数.

举出使

$$b^2-4ac=-3,\ -4,\ -7,\ -8$$

的二次型的例子.

举一个 $b^2-4ac=-4k$ 的二次型例子．

举一个 $b^2-4ac=-4k-3$ 的二次型例子．

41．设 $b^2-4ac=-4$，指出 b 的奇偶性．列出以 -4 为判别式且 $|b|\leqslant 10$ 的所有正定二次型，并证明它们都与 x^2+y^2 等价．

42．设 $b^2-4ac=-3$，指出 b 的奇偶性．列出以 -3 为判别式且 $|b|\leqslant 10$ 的所有正定二次型，并证明它们都与 x^2+xy+y^2 等价．

43．二次型 $2x^2+3y^2$ 与 x^2+6y^2 的判别式是什么？这两个二次型中的每一个可以表示出数 1，2，3，4，5，6，7 中的哪些？这两个二次型是否等价？

正规表示

若 $n=ax^2+bxy+cy^2$，则 $k^2n=a(kx)^2+b(kx)(ky)+c(ky)^2$，因此，若一个二次型能表示一个数，那么它就能表示这个数与任何平方数之积．这样，由二次型当 $\gcd(x,y)=1$ 时所取的数值就能推出它所可能取到的所有其余的数值.

44．对 (x,y) 分别做替换 $(x,x+y)$，$(x,2x+y)$，$(x,3x+y)$，$(x,4x+y)$ 以及 $(2x+y,3x+2y)$，求所得到的 x^2+y^2 的等价二次型．列出这些二次型中 x^2 的系数，并与 x^2+y^2 所可能取的、不超过 20 的数值比较．这两组数之间有何异同？

45．设 $(x,y)\to(px+ry,qx+sy)$ 是幺模变换，证明在 x^2+y^2 中用 $(px+ry,qx+sy)$ 替换 (x,y) 所得到的二次型中 x^2 的系数是 x^2+y^2 所取的某个值.

46．设 $(x,y)\to(px+ry,qx+sy)$ 是幺模变换．证明 $\gcd(p,q)=1$．若 $\gcd(p,q)=1$，是否可以找到 r 与 s，使得 $(x,y)\to(px+ry,qx+sy)$ 是幺模变换？（见问题 1.34）．

47．判定 20，26 及 29 能否是与 x^2+y^2 等价的某个二次型中 x^2 的系数．如果是，写出使 x^2+y^2 变为这样的二次型的替换．

$1^2+0^2=1$，　　$4^2+1^2=17$，

$1^2+1^2=2$，　　$3^2+3^2=18=3^2(1^2+1^2)$，

$2^2+0^2=4=2^2(1^2+0^2)$，　　$4^2+2^2=20=2^2(2^2+1^2)$，

$2^2+1^2=5$，　　$4^2+3^2=25=5^2+0^2=5^2(1^2+0^2)$，

$2^2+2^2=8=2^2(1^2+1^2)$，　　$5^2+1^2=26$，

$3^2+0^2=9=3^2(1^2+0^2)$，　　$5^2+2^2=29$，

$3^2+1^2=10$，　　$4^2+4^2=32=4^2(1^2+1^2)$，

$3^2+2^2=13$，　　$5^2+3^2=34$，

$4^2+0^2=16=4^2(1^2+0^2)$，　　$6^2+0^2=36=6^2(1^2+0^2)$.

48. 若 $\gcd(p,q)=1$ 及 $n=ap^2+bpq+cq^2$，则称整数 n 可用二次型 $ax^2+bxy+cy^2$ 正规表示. 若 p (或 q) $=0$，那么仅当 q (或 p) $=\pm1$ 时，n 是用这个二次型正规表示.

列出不超过 20 并且可以用二次型 x^2+y^2 正规表示的数.

49. 设 n 可用二次型 $ax^2+bxy+cy^2$ 正规表示，证明存在一个等价的二次型，其中 x^2 的系数是 n.

50. 设二次型 $ax^2+bxy+cy^2$ 与 $nx^2+hxy+ly^2$ 等价，证明 n 可用 $ax^2+bxy+cy^2$ 正规表示.

51. 设 $ax^2+bxy+cy^2$ 与 $a'x^2+b'xy+c'y^2$ 是等价的二次型，于是存在幺模矩阵 P，使得

$$P\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}P^{\mathrm{T}}=\begin{pmatrix} a' & \frac{1}{2}b' \\ \frac{1}{2}b' & c' \end{pmatrix},$$

再设 $n=ap^2+bpq+cq^2$ 且 $\gcd(p,q)=1$，求 n 用 $a'x^2+b'xy+c'y^2$ 的表示式，并利用问题 18 证明这是一个正规表示.

52. 若数 7 可用二次型 $x^2+xy+6y^2$ 表示 (若可表示，则必是正规表示，因为 7 是素数)，那么是否存在等价的二次型 $7x^2+hxy+ly^2$，其中 h，l 是整数？

通过对模 7 考虑这两个二次型的判别式，证明：若 7 可由 $x^2+xy+6y^2$ 表示，则将会推出矛盾.

约 化 型

现在，对于正定二次型，我们要对每类等价二次型确定一个标准形式（这种形式是唯一的）.

53. 计算 $x^2+xy+4y^2$ 与 $2x^2+xy+2y^2$ 的判别式. 对于 $|x|$，$|y|<3$，求它们的值. 试推测它们是否等价.

令 $f(x,y)=2x^2+xy+2y^2$，利用 $f(x,y)=2\left(x+\frac{1}{4}y\right)^2+\frac{15}{8}y^2$，证明当 $|y|\geqslant 2$ 时，$f(x,y)>7$.

再证明当 $|x|\geqslant 2$ 且 $y=\pm 1$ 时，$f(x,y)>7$.

推出 $2x^2+xy+2y^2$ 可以正规表示的最小的两个非零数是 2 和 3.

证明 $x^2+xy+4y^2$ 与 $2x^2+xy+5y^2$ 不等价.

54. 求可用 $2x^2+xy+5y^2$ 和 $3x^2+3xy+4y^2$ 正规表示的最小的几个非零数. 证明：这两个二次型的判别式虽然相同，却不等价.

55. 证明二次型 $ax^2+bxy+cy^2$ 可取值 a，c 及 $a+c-b$.

再证明：若 $0\leqslant b\leqslant a\leqslant c$ 且 $a>0$，则当 $|y|\geqslant 2$ 时，$ax^2+bxy+cy^2\geqslant 3c>a+c$. 此外，当 $y=\pm 1$ 且 $|x|\geqslant 2$ 时，$ax^2+bxy+cy^2\geqslant 2a+c>a+c$.

进而推出：在不超过 $a+c$ 的非零数中，能被正规表示的只有当 $(x,y)=(\pm 1,0)$，$(0,\pm 1)$ 或 $(\pm 1,\pm 1)$ 的时候，而这些数就是 a，c 和 $a+c-b$.

56. 设二次型 $ax^2+bxy+cy^2$ 与 $a'x^2+b'xy+c'y^2$ 是等价的，且 $0\leqslant b\leqslant a\leqslant c$，$0\leqslant b'\leqslant a'\leqslant c'$，证明 $a=a'$，$b=b'$，$c=c'$.

57. 若 $0\leqslant b\leqslant a\leqslant c$，则称正定二次型 $ax^2+bxy+cy^2$ 是约化二次型.

对于约化二次型，有 $b^2 \leqslant ac$．由此证明：若约化二次型的判别式为 -3，则 $ac \leqslant 1$．求判别式为 -3 的所有约化二次型．

58．求判别式为 -4，-12 的所有约化二次型．

59．证明：对于判别式为 $-d\,(<0)$ 的约化二次型，有 $ac \leqslant \frac{1}{3}d$．由此推出，具有任一给定的负判别式的约化型是有限个．

60．通过作替换 $(x, y) \to (x+y, y)$ 足够多次，找出与 $2x^2 - 11xy + 18y^2$ 等价的约化型．找出一个变换，把 $2x^2 - 11xy + 18y^2$ 变为与它等价的约化型．

61．通过作替换 $(x, y) \to (x-y, y)$ 足够多次，找出与 $2x^2 + 13xy + 24y^2$ 等价的约化型．找出一个变换，把 $2x^2 + 13xy + 24y^2$ 变为与它等价的约化型．

62．n 取什么值时，对 $3x^2 + 50xy + 211y^2$ 作替换 $(x, y) \to (x+ny, y)$ 后，xy 的系数的绝对值最小？

求与这个二次型等价的约化型．

63．n 取什么值时，对 $3x^2 + 47xy + 185y^2$ 作替换 $(x, y) \to (x+ny, y)$ 后，xy 的系数的绝对值最小？

求这个二次型的约化型（必要时，可再作替换 $(x, y) \to (y, x)$ 和 $(x, y) \to (-x, y)$）．

64．求等价于二次型 $3x^2 + 46xy + 177y^2$ 的约化型．

65．设替换 $(x, y) \to (x+ny, y)$ 将正定二次型 $ax^2 + bxy + cy^2$ 变换为 $a'x^2 + b'xy + c'y^2$．

证明 $a = a'$．而且，适当选取整数 n，可使 $|b'| \leqslant a$．

66．利用一系列形如 $(x, y) \to (x+ny, y)$，$(x, y) \to (y, x)$，$(x, y) \to (-x, y)$ 的替换（可以重复），说明正定二次型 $ax^2 + bxy + cy^2$ 等价于一个约化型．

67．证明：判别式为定值的正定二次型的等价类的个数有限．

68．在素数模 7，11，13，17 中，-2 是哪一个的二次剩余？

对于那些使 -2 成为二次剩余的素数 p（$=7, 11, 13, 17$），

求 h 与 l，使得 $h^2-pl=-2$，然后构造一个二次型，使其判别式为 -8，x^2 的系数为 p.

求出判别式为 -8 的所有约化型，并证明素数 7，11，13，17 都可用 x^2+2y^2 表示.

69. 对 $p\equiv 1,3,5,7 \pmod 8$，求 $\left(\frac{-2}{p}\right)$ 之值.（见问题 4.42）.

求出可用二次型 x^2+2y^2 表示的素数.

70. 利用等式 $(x^2+2y^2)(a^2+2b^2)=(xa+2yb)^2+2(xb-ya)^2$ 对所有能用 x^2+2y^2 表示的数做一个全面的描述.

71. 求判别式为 -20 的所有约化二次型.

构造一个判别式为 -20 且 x^2 系数为 30 的二次型. 证明 30 可以用二次型 x^2+5y^2 或 $2x^2+2xy+3y^2$ 正规表示.

72. 假设只有一个约化型的判别式是 b^2-4ac，试用二次同余式的可解性，给出正整数 n 可用 $ax^2+bxy+cy^2$ 正规表示的充要条件.

定二次型的自守变换

73. 对于哪些幺模变换

$$(x,y)\to(px+ry,\ qx+sy),$$

有

$$(px+ry)^2+2(qx+sy)^2=x^2+2y^2?$$

证明这四个幺模变换构成一个群，即 x^2+2y^2 的自守变换群.

74. 对于哪些幺模变换

$$(x,y)\to(px+ry,\ qx+sy),$$

有

$$(px+ry)^2+(qx+sy)^2=x^2+y^2?$$

证明这八个幺模变换构成一个群，即 x^2+y^2 的自守变换群.

75. 对于哪些幺模变换

$$(x,y)\to(px+ry,\ qx+sy),$$

有

$$(px+ry)^2+(px+ry)(qx+sy)+(qx+sy)^2=x^2+xy+y^2\ ?$$

证明这十二个变换构成一个群，即 x^2+xy+y^2 的自守变换群.

76. 求约化二次型 $ax^2+bxy+cy^2$ 的自守变换群：

(i) 若 $0=b<a<c$，

(ii) 若 $0<b\leqslant a<c$，

(iii) 若 $b=0$ 且 $a=c$，

(iv) 若 $0<b<a=c$，

(v) 若 $a=b=c$.

77. 设 A 是对称矩阵，P 和 M 是幺模矩阵，证明 $A=PAP^{\mathrm{T}}$ 的充要条件是

$$(MPM^{-1})MAM^{\mathrm{T}}(MPM^{-1})^{\mathrm{T}}=MAM^{\mathrm{T}}.$$

证明任何正定二次型的自守变换群与问题 76 中所得到的某个自守变换群同构.

注记与答案

参考书见书目:Davenport (1968).Niven与Zuckerman (1972).

1. 因为 τ 和 σ 都是平移，所以 $\tau^m\sigma^n(\Pi)$是平行四边形. 因为 τ 与 σ 是格平移，所以 $\tau^m\sigma^n(\Pi)$的顶点是格点.若在 $\tau^m\sigma^n(\Pi)$的内部或周界上有异于顶点的格点,则它们经平移 $\tau^{-m}\sigma^{-n}$ 后的像在 Π 的内部或其周界上.

2. 全体平行四边形 $\tau^m(\Pi)$覆盖了在两个方向都无界的一个带形. 因为 σ 平移的方向和 τ 平移的方向不平行，所以全体平移 σ^n 把这个无界带形又映射成一些平行的带形，它们在原带形的两边都是无界的；因此，平面的每个点被这些带形所覆盖. 特别地，每个格点被它们覆盖. 但是，格点不在平行四边形 $\tau^m\sigma^n(\Pi)$ 的内部或周界上 (除非是顶点)，这样，每个格点是 A，B，C 或 D 在平移 $\tau^m\sigma^n$ 下的像. 例如，设 C 是平行四边形 $ABCD$ 中与 A 相

对的顶点，若 $\tau^m\sigma^n(A)=P$，则 $\tau^{m-1}\sigma^n(B)=P$，$\tau^m\sigma^{n-1}(D)=P$，$\tau^{m-1}\sigma^{n-1}(C)=P$，从而 P 是四个平行四边形 $\tau^m\sigma^n(\Pi)$，$\tau^{m-1}\sigma^n(\Pi)$，$\tau^m\sigma^{n-1}(\Pi)$，$\tau^{m-1}\sigma^{n-1}(\Pi)$的顶点．

3． $C=(a+c,b+d)$．

经变换 α 后，单位正方形的像是平行四边形 $ABCD$，格点 $(x,0)$的像是直线 AB 上的格点，格点 $(0,y)$的像是直线 AD 上的格点，单位正方形格的像是单位平行四边形格．

4． 是（由问题 2 与问题 3）．

5． 过点 B，C，D 各作 x 轴的垂线，并计算由它们所构成的直角三角形和梯形的面积，可知这个平行四边形的面积是$|ad-bc|$．对于任何实数 a，b，c，d 这都正确．若平行四边形面积为零，则四个顶点共线．

数 $ad-bc$ 称为矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$的行列式．

6． $(ar+cs,br+ds)=(at+cu,bt+du)$

$$\Longleftrightarrow (a(r-t)+c(s-u),b(r-t)+d(s-u))=(0,0),$$

因此

$$\alpha:\quad (r-t,s-u)\to(0,0).$$

$$\alpha:\quad (0,y)\to(yc,yd)\text{，所以若 } y\neq0\text{，则}$$

$c=d=0$．

$$(ax+cy,bx+dy)=(0,0)\qquad(x\neq0)$$

$$\Rightarrow d(ax+cy)-c(bx+dy)=0,$$

即

$$(ad-bc)x=0.$$

但 $x\neq0$，所以

$$ad-bc=0.$$

若 α 不是一一对应的，则必有两个不同的点有相同的像．由上可知，两点的差是一个不同于原点的点，但在变换 α 下，这点的像却是原点．正如我们已经证明的，无论这点是否在 y 轴上，总可推出 $ad-bc=0$．

7． 问题 4 中已证明 α 是一个满射．

若 α 不是一一对应的，则由问题 6 得到 $ad-bc=0$，因而 A，B，C，D 这四个点共线．

8．若 a，b，c，d 是整数，则 $ad-bc$ 亦是．

$$\alpha:\left(\frac{d}{ad-bc},\ \frac{-b}{ad-bc}\right)\rightarrow(1,0).$$

$$\alpha:\left(\frac{-c}{ad-bc},\ \frac{a}{ad-bc}\right)\rightarrow(0,1).$$

但是 α 是 $\mathbf{Z}^2$ 到自身的双射，所以此处的四个坐标是整数，因此它们的积与和都是整数，从而

$$\frac{a}{ad-bc}\ \frac{d}{ad-bc}-\frac{b}{ad-bc}\ \frac{c}{ad-bc}$$

$$=\frac{ad-bc}{(ad-bc)^2}=\frac{1}{ad-bc}$$

是整数．但是，如果一个整数的倒数也是整数，它必是 ±1，所以 $ad-bc=\pm1$．

9．设 a，b，c，d 是整数，则变换就把 $\mathbf{Z}^2$ 内射到 $\mathbf{Z}^2$．

若 $ad-bc=\pm1$，则 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ 的逆矩阵

$$\begin{pmatrix}\dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc}\\[2ex] \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc}\end{pmatrix}$$

的元素是整数，因而每个格点都以一个格点为其原像．所以这个变换把 $\mathbf{Z}^2$ 满射到 $\mathbf{Z}^2$．

10．问题 1 — 8 的论证证明，这种平行四边形的面积等于 1．

11. 半周旋转把直线映射成平行的直线．关于点 M 的半周旋转将 B 与 C 交换位置，所以 $ABA'C$ 是平行四边形．若将这个格按通常办法用有序的整数对标出，那么点 M 的坐标是整数或整数 $+\frac{1}{2}$．若 $M=(r,s)$，关于 (r,s) 的半周旋转是 $(x,y)\to(-x+2r,-y+2s)$，它当然将 $\mathbf{Z}^2$ 映射到自身，所以 A' 是格点．因为半周旋转把格满射到自身，所以三角形 $A'BC$ 中的格点只能是 ABC 中的格点在半周旋转下的像．

12. $\frac{1}{2}$．问题11中构造的平行四边形面积二倍于三角形面积，等于1．

13. $0,\frac{1}{6},\frac{1}{5},\frac{1}{4},\frac{1}{3},\frac{2}{5},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},\frac{4}{5},\frac{5}{6},1$．

14. 若 $\frac{a}{b}$ 是 Farey 数列的一项，则 $\gcd(a,b)=1$，因而在连结 $(0,0)$ 和 (b,a) 的线段上无格点．同样地，在连结 $(0,0)$ 到 (d,c) 的线段上无格点．因为 $\frac{a}{b}$ 与 $\frac{c}{d}$ 是 Farey 数列中相邻两项，所以在连接 (b,a) 和 (d,c) 的线段上，以及在顶点为 $(0,0)$，(b,a)，(d,c) 的三角形内部都无格点．因此，这个三角形的面积是 $\frac{1}{2}$（由问题12），而且 $ad-bc=\pm 1$（由问题5）．

但是 $\frac{a}{b}<\frac{c}{d}$，所以 $ad<bc$，$ad-bc=-1$．

类似地，有 $cf-de=-1$．

于是 $ad-bc=cf-de$，$d(a+e)=c(b+f)$．

15. 幺模变换是正方形格的一个自同构，它以一个格点为不动点．单位正方形 $(0,0)$，$(1,0)$，$(1,1)$，$(0,1)$ 在这个变换之下

的像是 $(0,0)$，(p,q)，$(p+r,q+s)$，(r,s)，它们构成一个面积为 1 的平行四边形．

在专家们当中，几乎有一半人使用我们对幺模的定义，另一半人则只把行列式为 $+1$ 的矩阵称为幺模矩阵．

16. $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$的转置矩阵是 $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$，它们有相同的行列式，因而或者都是幺模矩阵，或者都不是．

当 $ps-qr=\pm 1$ 时，$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$的逆矩阵是 $\begin{pmatrix} \pm s & \mp q \\ \mp r & \pm p \end{pmatrix}$，它仍是幺模矩阵．

17. 显然单位矩阵是幺模矩阵，这样，根据问题 16，只需证明封闭性．

令 $ps-qr=\pm 1$ 且 $ad-bc=\pm 1$，则

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} pa+qc & pb+qd \\ ra+sc & rb+sd \end{pmatrix}.$$

最后一个矩阵的行列式是

$$(pa+qc)(rb+sd)-(ra+sc)(pb+qd)$$
$$=ps\cdot ad+qr\cdot bc+pr\cdot ab+qs\cdot cd-pr\cdot ab-ps\cdot bc-qr\cdot ad$$
$$-qs\cdot cd=ps\cdot ad+qr\cdot bc-ps\cdot bc-qr\cdot ad$$
$$=(ps-qr)(ad-bc)=\pm 1.$$

18. $\gcd(x,y)=\gcd(X,Y)$是因为它们互相整除．从几何上说，$\gcd(x,y)$是连结 $(0,0)$与(x,y)的线段上除点 $(0,0)$外的格点数．在幺模变换下，共线格点的集合被一一映射成共线格点的集合．

19. $(x,y)\to(x,y)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$是关于 x 轴的反射．

$(x,y)\to(x,y)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$是关于直线 $y=x$ 的反射．

$(x,y)\to(x,y)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$是关于原点的反时针旋转 90°．

$(x,y)\to(x,y)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$是沿 x 轴方向的切变[①]．

20. 行列式等于 $+1$ 的矩阵给出一个指数为 2 的子群．因为

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ a+b & 1 \end{pmatrix},$$

① “切变”原文为 shear．对这一变换的几何意义，可参见图 8.2．—— 译者注．

所以这些矩阵构成一个与$(\mathbf{Z}, +)$同构的群，相应的变换是沿 x 轴方向的切变．

21．$1^2+0^2=1$ ，　　$3^2+0^2=9$ ，

$1^2+1^2=2$ ，　　$3^2+1^2=10$ ，

$2^2+0^2=4$ ，　　$3^2+2^2=13$ ，

$2^2+1^2=5$ ，　　$3^2+3^2=18$ ，

$2^2+2^2=8$ ，

对于 $n=1, 2, 4, 5, 8, 9$ 的圆，见图 8.3．

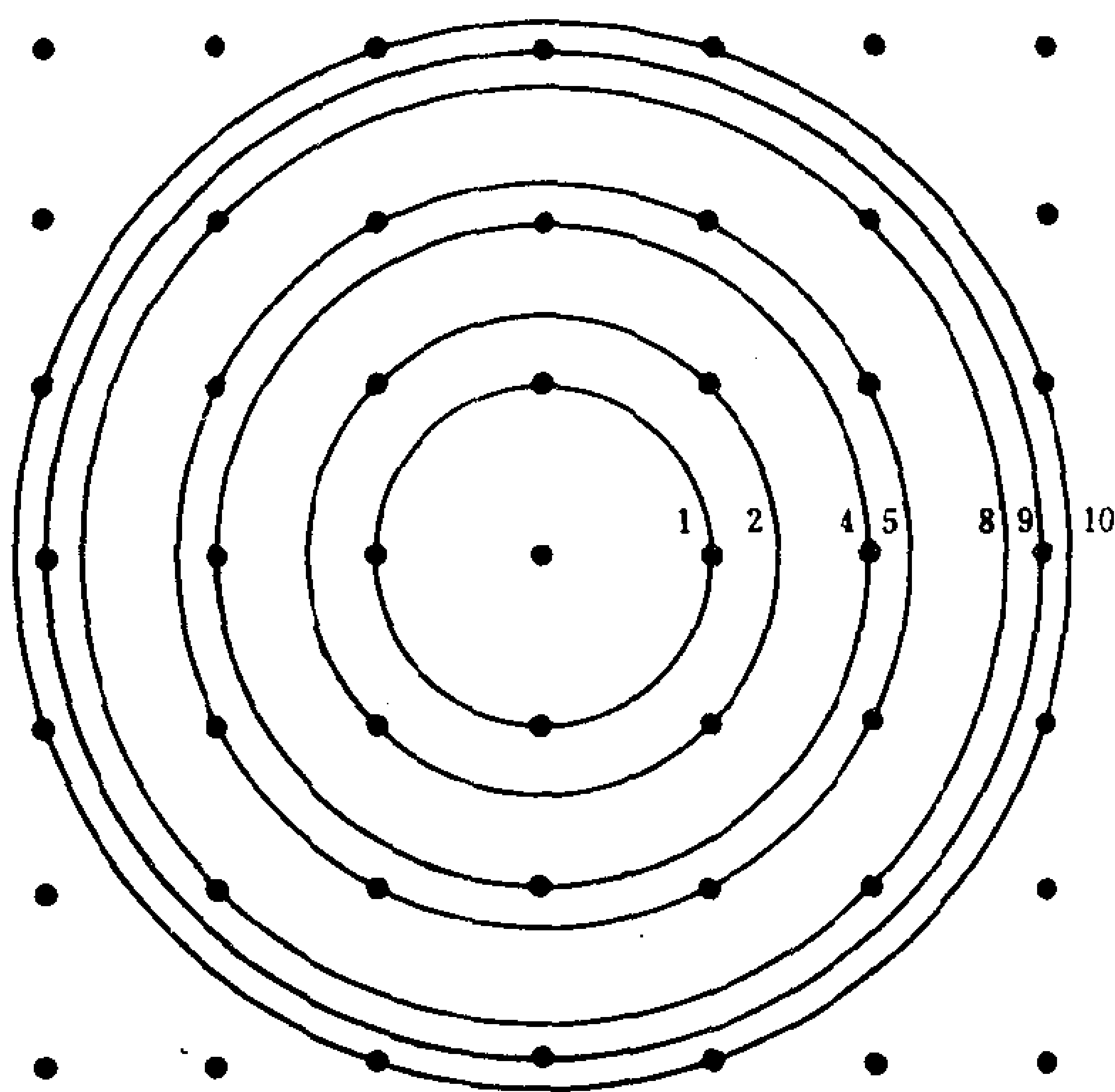


图 8.3

22．显然$(x+y)^2$与y^2只能是正数或零．但 $x+y$ 与 y 都是整数，所以只可能取问题 21 中的那些值．数 3 不是二平方之和．

23．若 $x=m-2n$ 且 $y=n$，则 $x+2y=m$，$y=n$．因此$(x+2y)^2+y^2$与m^2+n^2或x^2+y^2有相同的数值集合．

对于给定的 a, b, c，称 x 与 y 的函数$f(x, y)=ax^2+bxy+cy^2$为二元二次型．

24. 若 $ps-qr=\pm 1$ 且 p,q,r,s 都是整数，则存在格点 (x,y)，它被幺模变换

$$(x,y)\to(x,y)\begin{pmatrix}p & q\\ r & s\end{pmatrix}$$

映射到格点 $(px+ry,\ qx+sy)$. 因此，适当选择 x,y, 可使 $px+ry$ 与 $qx+sy$ 取到任何一对整数值.

25. $(a+b,b)$ 在圆 $x^2+y^2=25$ 上 $\Longleftrightarrow (a+b)^2+b^2=25$

$\Longleftrightarrow (a,b)$ 在曲线 $(x+y)^2+y^2=25$ 上.

$(x,y)\to(x+y,y)$ 是一个切变，它使 x 轴上的点保持不动，以及每一点沿着与 x 轴平行的方向移动，移动的距离等于它到 x 轴的距离.

虽说出于数论研究的目的，我们只关心变量 x,y 取整数值，因而只是圆 $x^2+y^2=25$ 上的几个点，但用通常方式画出圆和椭圆可以对某些二次型有个直观的模型. 因此，只要记住我们关心的主要是格点，就不会引起误解.

若有幺模变换将两个二次型中的一个变成另一个，则称它们是等价的. 由这个定义推出，等价二次型取相同的整数值集合. 另一个推论是，由于幺模变换构成一个群，所以这样定义的等价是通常意义下的一个等价关系，因而这个等价关系将所有二元二次型的集合分成不相交的类.

26. 因为 $x^2+2xy+2y^2=(x+y)^2+y^2$，所以当 $(a+b,b)$ 在 $x^2+y^2=k$ 上时，(a,b) 在 $x^2+2xy+2y^2=k$ 上. 这样，三个椭圆分别变换成三个圆：$x^2+y^2=9$，$x^2+y^2=16$ 与 $x^2+y^2=25$.

用将圆做切变的办法，画出草图.

27. $x^2-2xy+3y^2=(x-y)^2+2y^2$，

$x^2+2xy+3y^2=(x+y)^2+2y^2$，

$x^2+4xy+6y^2=(x+2y)^2+2y^2$.

三个变换：$(x,y)\to(x-y,y)$，

$(x,y)\to(x+y,y)$，

$(x,y)\to(x+2y,y)$

都是幺模变换，因而上面所给出的三个二次型都与 x^2+2y^2 等价．

28．$\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x+y\\y\end{pmatrix}$．

29．
$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\1&2\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\1&3\end{pmatrix}.$$

(a,b)在 $x^2+2xy+3y^2=k$ 上

$\Longleftrightarrow (a\quad b)\begin{pmatrix}1&1\\1&3\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}=k$

或
$$(a\quad b)\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}=k$$

或

$(a,b)\begin{pmatrix}1&0\\1&1\end{pmatrix}$在曲线 $(x\quad y)\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=k$ 上．

30．$(px+ry)^2+2(qx+sy)^2=(x\quad y)\begin{pmatrix}p&q\\r&s\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}p&r\\q&s\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$.

31．$P=\begin{pmatrix}p&q\\r&s\end{pmatrix}$．

这个结果，用代数语言说明了等价二次型之间是如何通过幺模变换相联系的．

32．$x^2-2xy+3y^2=(x\quad y)\begin{pmatrix}1&-1\\-1&3\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$，行列式 $=2$．

$x^2+2y^2=(x\quad y)\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$，行列式 $=2$.

$x^2+2xy+3y^2=(x\quad y)\begin{pmatrix}1&1\\1&3\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$，行列式 $=2$.

$x^2+4xy+6y^2=(x\quad y)\begin{pmatrix}1&2\\2&6\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$，行列式 $=2$．

33．在注记 17 中，“矩阵是幺模的”这个条件，是在证明了我们这里所需要的结果后才加上去的．因此，$\det PAP^{\mathrm{T}}=(\det P)\cdot(\det A)(\det P^{\mathrm{T}})$．但是 $\det P=\det P^{\mathrm{T}}$ 对一切 P 都成立，所以，若 P 是幺模矩阵，则 $\det P=\pm 1$．于是 $(\det P)(\det P^{\mathrm{T}})=1$，$\det PAP^{\mathrm{T}}=\det A$．

34．若这两个二次型等价，则对于某个幺模矩阵 P，有 $B=PAP^{\mathrm{T}}$．由上题得到 $\det B=\det A$．

35．$ax^2+bxy+cy^2=(x\quad y)\begin{pmatrix}a&\frac{1}{2}b\\\frac{1}{2}b&c\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$．$2\times 2$ 阶对称矩阵的行列式是 $ac-\frac{1}{4}b^2$．因此，$ac-\frac{1}{4}b^2=a'c'-\frac{1}{4}b'^2$，即

$b^2-4ac=b'^2-4a'c'$.

36. x^2+y^2，$b^2-4ac=-4$，$x^2+y^2=1$ 是圆.

x^2，$b^2-4ac=0$，$x^2=1$ 是一对平行直线.

x^2-y^2，$b^2-4ac=4$，$x^2-y^2=1$ 是等轴双曲线.

本题的目的是说明 b^2-4ac 符号的变化引起的二次型的差别.

37. 判别式等于 -4 乘以相应矩阵的行列式. 若 $b^2-4ac<0$，则 $4ac-b^2>0$，$(4ac-b^2)y^2$ 是正数或零. 这样，右边是正数或零，因而 $4a$ 和 $ax^2+bxy+cy^2$ 必同号.

38. 正定二次型总取非负值，且对应着一族同心椭圆.

负定二次型总取非正值.

等价的二次型有相同的判别式，所以等价于定二次型的二次型也是定二次型. 此外，等价的二次型取相同的整数值集合，所以，或者都是正的，或者都是负的. 这样，前面所定义的二次型的等价也是在正定二次型集合中的一个等价关系.

39. x^2-y^2 当 $y=0$ 时取正值，当 $x=0$ 时取负值.

对于一切的 $(0,y)$，x^2 为 0.

40. 若 b 是偶数，$b^2\equiv 0 \pmod 4$，所以 $b^2-4ac\equiv 0 \pmod 4$.

若 b 是奇数，$b^2\equiv 1 \pmod 4$，所以 $b^2-4ac\equiv 1 \pmod 4$.

-1 与 -2 都不同余于 0 或 1 (mod 4)，但是对于任何 a,b,c，有 $b^2-4ac\equiv 0$ 或 1 (mod 4)，所以判别式不能是 $-1,-2,-5,-6,-9,-10$ 等等.

$b^2-4ac=-3$	x^2+xy+y^2
$b^2-4ac=-4$	x^2+y^2
$b^2-4ac=-7$	$x^2+xy+2y^2$
$b^2-4ac=-8$	x^2+2y^2
$b^2-4ac=-4k$	x^2+ky^2
$b^2-4ac=-4k-3$	$x^2+xy+(k+1)y^2$.

41. 若 $b^2-4ac=-4$，则 $b^2=4(ac-1)$，所以 b 是偶数.

$b=0 \Rightarrow ac=1 \Rightarrow a=1$ ， x^2+y^2

$b=\pm 2 \Rightarrow ac=2$ $x^2\pm 2xy+2y^2=(x\pm y)^2+y^2$ ，

$\Rightarrow a=1$ 或 2 $2x^2\pm 2xy+y^2=x^2+(x\pm y)^2$.

$b=\pm 4 \Rightarrow ac=5$ $x^2\pm 4xy+5y^2=(x^2\pm 2y)^2+y^2$,

$\Rightarrow a=1$ 或 5 $5x^2\pm 4xy+y^2=x^2+(x\pm 2y)^2$.

$b=\pm 6 \Rightarrow ac=10$ $x^2\pm 6xy+10y^2=(x\pm 3y)^2+y^2$,

$\Rightarrow a=1,2,5,10$ $2x^2\pm 6xy+5y^2=(x\pm y)^2+(x\pm 2y)^2$,

$5x^2\pm 6xy+2y^2=(x\pm y)^2+(2x\pm y)^2$,

$10x^2\pm 6xy+y^2=x^2+(3x^2\pm y)^2$.

$b=\pm 8 \Rightarrow ac=17$ $x^2\pm 8xy+17y^2=(x\pm 4y)^2+y^2$,

$\Rightarrow a=1, 17$ $17x^2\pm 8xy+y^2=x^2+(4x\pm y)^2$.

$b=\pm 10 \Rightarrow ac=26$ $x^2\pm 10xy+26y^2=(x\pm 5y)^2+y^2$,

$\Rightarrow a=1,2,13,26$ $2x^2\pm 10xy+13y^2=(x\pm 2y)^2+(x\pm 3y)^2$,

$13x^2\pm 10xy+2y^2=(2x\pm y)^2+(3x\pm y)^2$,

$26x^2\pm 10xy+y^2=x^2+(5x\pm y)^2$.

42. $b^2=4ac-3$，所以 b 是奇数．

$b=\pm 1 \Rightarrow ac=1$ $x^2\pm xy+y^2=x^2+x(\pm y)+(\pm y)^2$.

$\Rightarrow a=1$

$b=\pm 3 \Rightarrow ac=3$ $x^2\pm 3xy+3y^2=(x\pm y)^2+(x\pm y)(\pm y)+(\pm y)^2$,

$\Rightarrow a=1$ 或 3 $3x^2\pm 3xy+y^2=(\pm x)^2+(\pm x)(x\pm y)+(x\pm y)^2$.

$b=\pm 5 \Rightarrow ac=7$ $x^2\pm 5xy+7y^2$

$\Rightarrow a=1$ 或 7 $=(x\pm 2y)^2+(x\pm 2y)(\pm y)+(\pm y)^2$,

$7x^2\pm 5xy+y^2$

$=(\pm x)^2+(\pm x)(2x\pm y)+(2x\pm y)^2$.

$b=\pm 7 \Rightarrow ac=13$ $x^2\pm 7xy+13y^2$

$\Rightarrow a=1$ 或 13 $=(x\pm 3y)^2+(x\pm 3y)(\pm y)+(\pm y)^2$,

$13x^2\pm 7xy+y^2$

$=(\pm x)^2+(\pm x)(3x\pm y)+(3x\pm y)^2$.

$b=\pm 9 \Rightarrow ac=21$ $\quad x^2 \pm 9xy+21y^2$

$\Rightarrow a=1,3,7$或21 $\quad = (x\pm 4y)^2+(x\pm 4y)(\pm y)+(\pm y)^2$,

$3x^2 \pm 9xy+7x^2$

$= (x\pm 2y)^2+(x\pm 2y)(x\pm y)+(x\pm y)^2$,

$7x^2 \pm 9xy+3y^2$

$= (x\pm y)^2+(x\pm y)(2x\pm y)+(2x\pm y)^2$,

$21x^2 \pm 9xy+y^2$

$= (\pm x)^2+(\pm x)(4x\pm y)+(4x\pm y)^2$.

43. $2x^2+3y^2$ 可取值2,3,5 但不能取 1,4,6,7.

x^2+6y^2 可以取值 1,4,6,7,但不能取 2,3,5.

尽管这两个二次型的判别式都是 -24,却不是等价的,因为他们的值集合不同.

因此,有相同的判别式是两个二次型等价的必要条件而非充分条件.

44. x^2+y^2 可以取到的值是 1,2,4,5,8,9,10,13,16,17,18,20.

x^2 的系数是 2,5,10,17,13.

这些系数是可取值集合的子集.

45. $(px+ry)^2+(qx+sy)^2=(p^2+q^2)x^2+2(pr+qx)xy+(r^2+s^2)y^2$.

46. 如果是幺模变换,则$px-qr=\pm 1$,所以$\gcd(p,q)=1$.若$\gcd(p,q)=1$,则由问题1.34,存在整数 s 与 r,使得$ps-qr=1$,因而 $(x,y)\to(px+ry,qx+sy)$是幺模变换.

47. $(5x+4y)^2+(x+y)^2=26x^2+42xy+17y^2$,

$(5x+2y)^2+(2x+y)^2=29x^2+24xy+5y^2$.

48. 1,2,5,10,13,17.

49. 若n 可由$ax^2+bxy+cy^2$正规表示,则 $n=ap^2+bpq+cq^2$,其中 $\gcd(p,q)=1$.根据问题 46,存在幺模变换 $(x,y)\to$

$(px+ry, qx+sy)$，于是 $ax^2+bxy+cy^2$ 等价于

$$a(px+ry)^2+b(px+ry)(qx+sy)+c(qx+sy)^2$$
$$=(ap^2+bpq+cq^2)x^2+\cdots=nx^2+\cdots.$$

50．若 $ax^2+bxy+cy^2$ 与 $nx^2+hxy+ly^2$ 等价，则存在幺模变换 $(x,y)\to(px+ry, qx+sy)$，

使得 $a(px+ry)^2+b(px+ry)(qx+sy)+c(qx+sy)^2$
$=nx^2+hxy+ly^2$.

因此 $n=ap^2+bpq+cq^2$.

因为是幺模变换，所以 $\gcd(p,q)=1$，n 被正规表示．

51．因为

$$P\begin{pmatrix}a & \frac{1}{2}b\\ \frac{1}{2}b & c\end{pmatrix}P^{\mathrm{T}}=\begin{pmatrix}a' & \frac{1}{2}b'\\ \frac{1}{2}b' & c'\end{pmatrix},$$

所以

$$\begin{pmatrix}a & \frac{1}{2}b\\ \frac{1}{2}b & c\end{pmatrix}=P^{-1}\begin{pmatrix}a' & \frac{1}{2}b'\\ \frac{1}{2}b' & c'\end{pmatrix}P^{-1\mathrm{T}},$$

因此

$$n=(p\ \ q)\begin{pmatrix}a & \frac{1}{2}b\\ \frac{1}{2}b & c\end{pmatrix}\begin{pmatrix}p\\ q\end{pmatrix}=(p\ \ q)P^{-1}\begin{pmatrix}a' & \frac{1}{2}b'\\ \frac{1}{2}b' & c'\end{pmatrix}P^{-1\mathrm{T}}\begin{pmatrix}p\\ q\end{pmatrix}.$$

若 $(p,q)P^{-1}=(X,Y)$，则 $n=a'X^2+b'XY+c'Y^2$ 是一个正规表示式（由问题18）．

52．由问题49知，必有一个等价二次型 $7x^2+hxy+ly^2$．

等价的二次型有相同的判别式，所以 $h^2-28l=1-24$，即 $h^2=5+7(4l-4)$，$h^2\equiv 5 \pmod 7$．但5不是对模7的二次剩余．

53．在每种情形，判别式都是 -15．

令 $g(x,y)=x^2+xy+4y^2$，$f(x,y)=2x^2+xy+2y^2$．

当 $|x|,|y|<3$ 时，$g(x,y)=0,1,4,6,10,15,16,19,24$ 而 $f(x,y)=0,2,3,5,8,12,20$．

当 $|y|\geqslant 2$ 时，$\frac{15}{8}y^2\geqslant\frac{15}{2}$，所以 $f(x,y)>7$．

当 $y=\pm1$ 时，$f(x,y)=2\left(x\pm\frac{1}{4}\right)^2+\frac{15}{8}$，因此，若

$|x|\geqslant2$，则 $f(x,y)\geqslant2\left(\frac{7}{4}\right)^2+\frac{15}{8}=8$.

当 $y=0$ 时，由于是正规表示，应有 $x=\pm1$. 因此，为了使 $f(x,y)<8$，$|x|$ 与 $|y|$ 都应小于 2，而这些情形已在前面列出来了.

$g(x,y)=\left(x+\frac{1}{2}y\right)^2+\frac{15}{4}y^2$，所以当 $|y|\geqslant2$ 时应有 $g(x,y)\geqslant15$.

当 $y=\pm1$ 时，$g(x,y)=\left(x\pm\frac{1}{2}\right)^2+\frac{15}{4}$，所以若还有

$|x|\geqslant2$，则 $g(x,y)\geqslant\left(\frac{3}{2}\right)^2+\frac{15}{4}=6$.

当 $y=0$ 时，由于是正规表示，应有 $x=\pm1$. 因此，为使 $g(x,y)$ 正规表示的值小于 6，$|x|$ 与 $|y|$ 都应小于 2，这些情况已见于前面. 这就证明了，由 f 和 g 正规表示的最小几个非零数是不同的，所以它们不等价.

54. 令 $f(x,y)=2x^2+xy+5y^2=2\left(x+\frac{1}{4}y\right)^2+\frac{39}{8}y^2$.

当 $|y|\geqslant2$ 时，$f(x,y)\geqslant\frac{39}{2}$.

当 $|x|\geqslant2$ 时，$f(x,\pm1)=2\left(x\pm\frac{1}{4}\right)^2+\frac{39}{8}\geqslant2\left(\frac{7}{4}\right)^2$

$+\dfrac{39}{8}=11.$

当 $y=0$ 时，由于是正规表示，应有 $x=\pm1$.因此，要使 $f(x,y)$ 正规表示的值小于11，则 $|x|$ 与 $|y|$ 都应小于2 .

$f(\pm1,0)=2$，$f(0,\pm1)=5$，$f(\pm1,\pm1)=8$，$f(\pm1,\mp1)=6$.

令 $g(x,y)=3x^2+3xy+4y^2=3\left(x+\dfrac{1}{2}y\right)^2+\dfrac{13}{4}y^2$. 当 $|y|\geqslant2$ 时，$g(x,y)\geqslant13$.

当 $|x|\geqslant2$ 时，

$$g(x,\pm1)=3\left(x\pm\frac{1}{2}\right)^2+\frac{13}{4}\geqslant3\left(\frac{3}{2}\right)^2+\frac{13}{4}=10.$$

当 $y=0$ 时，由于是正规表示，应有 $x=\pm1$. 因此，要使 $g(x,y)$ 正规表示的值小于10，$|x|$ 与 $|y|$ 都应小于2 .

$g(\pm1,0)=3$，$g(0,\pm1)=4$，$g(\pm1,\pm1)=10$，
$g(\pm1,\mp1)=4$.

这证明了，f 与 g 所取的最小几个非零值不同，所以，它们不等价 .

55． 令 $f(x,y)=ax^2+bxy+cy^2$，则 $f(1,0)=a$，$f(0,1)=c$，$f(1,-1)=a+c-b$.

当 $0\leqslant b\leqslant a\leqslant c$，$a>0$ 且 $|y|\geqslant2$ 时，

$$f(x,y)=a\left(x+\frac{b}{2a}y\right)^2+\left(c-\frac{b^2}{4a}\right)y^2\geqslant\left(c-\frac{b^2}{4a}\right)4.$$

但 $\dfrac{b^2}{a}\leqslant c$，所以 $f(x,y)\geqslant3c>a+c$.

当 $|x|\geqslant2$ 时，$f(x,\pm1)=a\left(x\pm\dfrac{b}{2a}\right)^2+c-\dfrac{b^2}{4a}$

$$\geqslant a\left(\frac{3}{2}\right)^2+c-\frac{1}{4}b\geqslant 2a+c.$$

当 $|x|\geqslant 2$ 时，$f(x,0)$ 不是正规表示，所以，对于小于 $a+c$ 且可用 f 正规表示的数，$|x|$ 与 $|y|$ 都应小于 2.

$f(\pm1,0)=a$，$f(0,\pm1)=c$，$f(\pm1,\pm1)=a+b+c$，$f(\pm1,\mp1)=a-b+c$.

56. 若两个二次型等价，则由问题 51,它们正规表示同样的数值集合，因此有相同的几个最小值. 这样，根据问题 55,$a=a'$，$c=c'$ 而且 $a-b+c=a'-b'+c'$，从而 $b=b'$.这证明了，至多有一个约化型与给定的二次型等价. 下面的十个问题将证明每个正定二次型与一个约化型等价.

57. 由 $0\leqslant b\leqslant a\leqslant c$ 可推出 $b^2\leqslant ac$.

若 $b^2-4ac=-3$，则 $4ac-3\leqslant ac$，$ac\leqslant 1$，因而有 $a=c=1$. $b^2-4=-3$ 导出 $b^2=1$，所以判别式等于 -3 的约化型只是 x^2+xy+y^2.

58. 若 $b^2-4ac=-4$，且 $b^2\leqslant ac$，则 $4ac-4\leqslant ac$，$3ac\leqslant 4$，因而 $a=c=1$，于是 $b^2=0$. 判别式等于 -4 的约化型只是 x^2+y^2. 若 $b^2-4ac=-12$，且 $b^2\leqslant ac$，则 $4ac-12\leqslant ac$，$3ac\leqslant 12$，$ac\leqslant 4$. 因为 $a^2\leqslant ac$，所以 $a=1$ 或者 $a=2$.

a	c	$b^2=4ac-12$	b	
1	1	-8	—	
1	2	-4	—	
1	3	0	0	x^2+3y^2
1	4	4	$2>1$	非约化的
2	1	非约化的		
2	2	4	2	$2x^2+2xy+2y^2$

59. 若 $b^2-4ac=-d$ 且 $b^2\leqslant ac$，则 $4ac-d\leqslant ac$，$3ac\leqslant d$

及 $ac \leqslant \frac{1}{3}d$. 所以 $c \leqslant \frac{1}{3}d$. 又由 $0 \leqslant b \leqslant a \leqslant c$，可知判别式等于 $-d$ 的约化型至多是有限个. 在 Davenport 的书 (1968) 中列出了判别式取值 -3 到 -83 的所有约化型. Davenport 把满足 $0 \leqslant |b| \leqslant a \leqslant c$ 的二次型称为约化型, 这是因为在他的幺模变换定义中，行列式要等于 $+1$.

60. $2(x+y)^2-11(x+y)y+18y^2=2x^2-7xy+9y^2$.

$2(x+y)^2-7(x+y)y+9y^2=2x^2-3xy+4y^2$.

$2(x+y)^2-3(x+y)y+4y^2=2x^2+xy+3y^2$，约化型.

$2(x+3y)^2-11(x+3y)y+18y^2=2x^2+xy+3y^2$.

因为 $(x,y)\begin{pmatrix}1&0\\1&1\end{pmatrix}=(x+y,y)$，而且 $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ 是幺模矩阵，所以用这个替换得到等价的约化型.

$(x,y)\begin{pmatrix}1&0\\3&1\end{pmatrix}=(x+3y,y)$，而 $\begin{pmatrix}1&0\\3&1\end{pmatrix}$ 也是幺模矩阵.

61. $2(x-y)^2+13(x-y)y+24y^2=2x^2+9xy+13y^2$.

$2(x-y)^2+9(x-y)y+13y^2=2x^2+5xy+6y^2$.

$2(x-y)^2+5(x-y)y+6y^2=2x^2+xy+3y^2$，是约化型.

$2(x-3y)^2+13(x-3y)y+24y^2=2x^2+xy+3y^2$.

$(x,y)\begin{pmatrix}1&0\\-1&1\end{pmatrix}=(x-y,y)$，而 $(x,y)\begin{pmatrix}1&0\\-3&1\end{pmatrix}=(x-3y,y)$.

$\begin{pmatrix}1&0\\-1&1\end{pmatrix}$ 与 $\begin{pmatrix}1&0\\-3&1\end{pmatrix}$ 都是幺模矩阵.

62. $3(x+ny)^2+50(x+ny)y+211y^2$

$=3x^2+(6n+50)xy+(3n^2+50n+211)y^2$.

当 $n=-8$ 时，$6n+50$ 有最小绝对值.

$3(x-8y)^2+50(x-8y)y+211y^2=3x^2+2xy+3y^2$，是约化型.

$(x,y)\begin{pmatrix}1&0\\-8&1\end{pmatrix}=(x-8y,y)$，$\begin{pmatrix}1&0\\-8&1\end{pmatrix}$ 是幺模矩阵.

63. $3(x+ny)^2+47(x+ny)y+185y^2$

$=3x^2+(6n+47)xy+(3n^2+47n+185)y^2$.

当 $n=-8$ 时，$6n+47$ 有最小绝对值.

$3(x-8y)^2+47(x-8y)y+185y^2=3x^2-xy+y^2$，不是约化型.

用 (y,x)替换 (x,y)，

$3x^2-xy+y^2$ 等价于 $x^2-xy+3y^2$，

再用 $(-x,y)$替换 (x,y)，

$x^2-xy+3y^2$ 等价于 $x^2+xy+3y^2$，是约化型.

$(x,y)\begin{pmatrix}1 & 0\\ -8 & 1\end{pmatrix}=(x-8y,y)$，$(x,y)\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=(y,x)$，

$(x,y)\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=(-x,y)$.

矩阵 $\begin{pmatrix}1 & 0\\ -8 & 1\end{pmatrix}$，$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$，$\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$都是幺模矩阵.

$\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ -8 & 1\end{pmatrix}=\begin{pmatrix}8 & -1\\ 1 & 0\end{pmatrix}$，$(x,y)\begin{pmatrix}8 & -1\\ 1 & 0\end{pmatrix}=(8x+y,-x)$.

$3(8x+y)^2+47(8x+y)(-x)+185(-x)^2=x^2+xy+3y^2$.

64. $3(x-8y)^2+46(x-8y)y+177y^2=3x^2-2xy+y^2$. 用 (y,x)替换 (x,y)，得到等价的型 $x^2-2xy+y^2$.

$(x+y)^2-2(x+y)y+3y^2=x^2+2y^2$，是约化型.

65. 由于 $a(x+ny)^2+b(x+ny)y+cy^2=ax^2+(2an+b)xy+(an^2+bn+c)y^2$，所以 $a=a'$. 因为 $-a+1,-a+2,\cdots,-1,0,1,\cdots,a-1,a$ 构成模 $2a$ 的完全剩余系，所以在 $-a+1$ 与 a 之间恰有一个整数同余于 $b\pmod{2a}$. 选取 n，使得 b'等于这个整数.

66. 根据问题 65，可以将 $ax^2+bxy+cy^2$ 变换为 $ax^2+b'xy+c'y^2$，其中 $|b'|\leqslant a$.

用 $(-x,y)$替换 (x,y)(如果这是必要的话)，得到等价的型 $ax^2+|b'|xy+c'y^2$. 若 $a\leqslant c'$，这就是一个约化型. 若 $a>c'$，则利用 (y,x)替换 (x,y)，得到等价的型 $c'x^2+|b'|xy+ay^2$.

若 $|b'|\leqslant c'$，得到的是约化型. 若 $|b'|>c'$，利用问题 65 中的替换与方法可以得到一个等价的型 $c'x^2+b''xy+a'y^2$，其中 $|b''|<c'$. 用$(-x,y)$替换 (x,y) (如果必要的话)，可得到等价型 $c'x^2+|b''|xy+a'y^2$.

若 $a'\geqslant c'$，得到的是约化型. 否则，可以再重复上面的过程. 因为 x^2 与 y^2 的系数都是正的，而每一次都使这些系数减小，所以

这种过程不会无限地重复下去，最后必得到一个约化型.

67. 由问题 56 知，每个等价类至多含有一个约化型．由问题 66 知，每个等价类又至少含有一个约化型．因此，每个等价类恰有一个约化型. 所要的结论可由问题 59 得出．

68. 见表 3.2 与问题 4.42；-2 是模 11 与模 17 的二次剩余. $3^2-11\cdot 1=-2$，$7^2-17\cdot 3=-2$. 因此 $6^2-4\cdot 11\cdot 1=-8$，$14^2-4\cdot 17\cdot 3=-8$，故所求的二次型是 $11x^2+6xy+y^2$ 与 $17x^2+14xy+3y^2$. 若 $ax^2+bxy+cy^2$ 是约化型，判别式为 -8，即 $b^2-4ac=-8$，那么，由 $b^2=4ac-8$ 及 $b^2\leqslant ac$ 推出 $ac\leqslant \dfrac{8}{3}$，所以 $a=1$，$c=1$ 或 2. 但是 $a=c=1$ 推出 $b^2-4=-8$，这不可能. 而 $a=1$，$c=2$ 推出 $b=0$. 所以判别式为 -8 的约化型只有 x^2+2y^2. 这样，前面的两个二次型一定与它等价，所以 11 与 17 都可用 x^2+2y^2 表示．

69. 由问题 4.42 知，

$$\left(\frac{-2}{p}\right)=1\text{，当 } p\equiv 1 \text{ 或 } 3 \pmod 8\text{，}$$

$$\left(\frac{-2}{p}\right)=-1\text{，当 } p\equiv 5 \text{ 或 } 7 \pmod 8\text{.}$$

如果有一个判别式等于 -8 的二次型 $px^2+hxy+ly^2$，即如果有整数 h，l，使得 $h^2-4pl=-8$，那么，因为 x^2+2y^2 是判别式等于 -8 的唯一的约化型，所以 p 可用它表示．为此，h 应是偶数，并且 $\left(\dfrac{1}{2}h\right)^2-pl=-2$，所以 -2 必是对模 p 的二次剩余．

反之，若 -2 是对模 p 的二次剩余，则存在 h，l，使得 $h^2-pl=-2$. 因而二次型 $px^2+2hxy+ly^2$ 的判别式为 -8. 因为这个型与 x^2+2y^2 等价，所以 p 可用 x^2+2y^2 表示．

70. 给出的等式表明，这个集合对乘法是封闭的．显然任何平方数都可用这个型表示．由问题 69 知，凡同余于 1 或 3 (mod 8) 的素数 p 和数 2 也都可用它表示．这样，一个整数，在它的素因数分解式中，只要同余于 5 或 7 (mod 8)的素因数的指数是偶数，就可以用这个型表示．若 $q \mid x^2+2y^2$，q 是同余于 5 或 7 (mod 8) 的素数，则 y 必有因数 q，因为，否则就存在 z，使得 $yz \equiv 1 \pmod{q}$，$(zx)^2+2 \equiv 0 \pmod{q}$，于是 -2 就成了对模 q 的二次剩余．这样，在那些可以表示的数的素因数分解式中，同余于5 或 7 (mod 8)的素因数的指数必是偶数．

71. 若 $ax^2+bxy+cy^2$ 是判别式为 -20 的约化二次型，则 $b^2-4ac=-20$，$b^2 \leqslant ac$，于是 $4ac-20 \leqslant ac$，$ac \leqslant 6$，$4ac \leqslant 24$．从而 $b^2 \leqslant 4$．

若 $b=0$，则 $ac=5$，从而 $a=1$，$c=5$．

若 $b=1$，则 $4ac=21$，这不可能．

若 $b=2$，则 $4ac=24$，从而 $ac=6$．由于 $b \leqslant a \leqslant c$，所以 $a=2$，$c=3$．

判别式为 -20 的两个约化型是 x^2+5y^2 与 $2x^2+2xy+3y^2$．

$30x^2+10xy+y^2$ 的判别式是 -20，所以它与上述两个型之一等价．于是 30 可用其中的一个正规表示．事实上，$5^2+5\cdot 1^2=30$．

72. n 可由 $ax^2+bxy+cy^2$ 正规表示的充要条件，是存在一个等价的二次型 $nx^2+hxy+ly^2$．若判别式等于 b^2-4ac 的约化型只有一个，则具有这一判别式的所有正定二次型都是等价的．因此，若有整数 h，l，使得

$$h^2-4nl=b^2-4ac,$$

则 n 是可表示的．若

$$h^2 \equiv b^2-4ac \pmod{4n},$$

即若 b^2-4ac 是对模 $4n$ 的二次剩余，那么这样的 h，l 是存在的．

73. $p=\pm 1$，$q=0$，$r=0$，$s=\pm 1$ 对应四个矩阵：

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\ \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix},$$

与 $C_2\times C_2$ 同构.

74. $p=\pm1$, $q=0$, $r=0$, $s=\pm1$ 或 $p=0$, $q=\pm1$, $r=\pm1$, $s=0$, 对应八个矩阵:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ \begin{pmatrix}1&0\\0&-1\end{pmatrix},\ \begin{pmatrix}-1&0\\0&1\end{pmatrix},\ \begin{pmatrix}0&1\\1&0\end{pmatrix},$$
$$\begin{pmatrix}0&-1\\-1&0\end{pmatrix},\ \begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \begin{pmatrix}0&-1\\1&0\end{pmatrix},$$

与 D_4 同构.

75. 由问题 55 知,当 $|x|,|y|\leqslant1$ 时, $ax^2+bxy+cy^2$ 取到它正规表示的最小值,因此,仅当 $(p,q)=(\pm1,0)$, $(0,\pm1)$ 或 $(\pm1,\mp1)$ 时才有 $p^2+pq+q^2=1$.

当 $(p,q)=(1,0)$ 时, $2r+s=1$ 且 $r^2+rs+s^2=1$,所以 $(r,s)=(0,1)$ 或 $(1,-1)$.

当 $(p,q)=(-1,0)$ 时, $-2r-s=1$,所以 $(r,s)=(0,-1)$ 或 $(-1,1)$.

当 $(p,q)=(0,1)$ 时, $r+2s=1$,所以 $(r,s)=(1,0)$ 或 $(-1,1)$.

当 $(p,q)=(0,-1)$ 时, $-r-2s=1$,所以 $(r,s)=(-1,0)$ 或 $(1,-1)$.

当 $(p,q)=(1,-1)$ 时, $r-s=1$,所以 $(r,s)=(1,0)$ 或 $(0,-1)$,

当 $(p,q)=(-1,1)$ 时, $-r+s=1$,所以 $(r,s)=(-1,0)$ 或 $(0,1)$.

矩阵 $\begin{pmatrix}1&-1\\1&0\end{pmatrix}$ 的阶数是 6, $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 的阶数是 2,生成群 D_6.

76. (i) 自守变换群有四个元素,与问题 73 中的群同构.

(ii) 自守变换群有两个元素,即单位元素和 $(x,y)\to(-x,-y)$.

(iii) 自守变换群有八个元素,与问题 74 中的群同构.

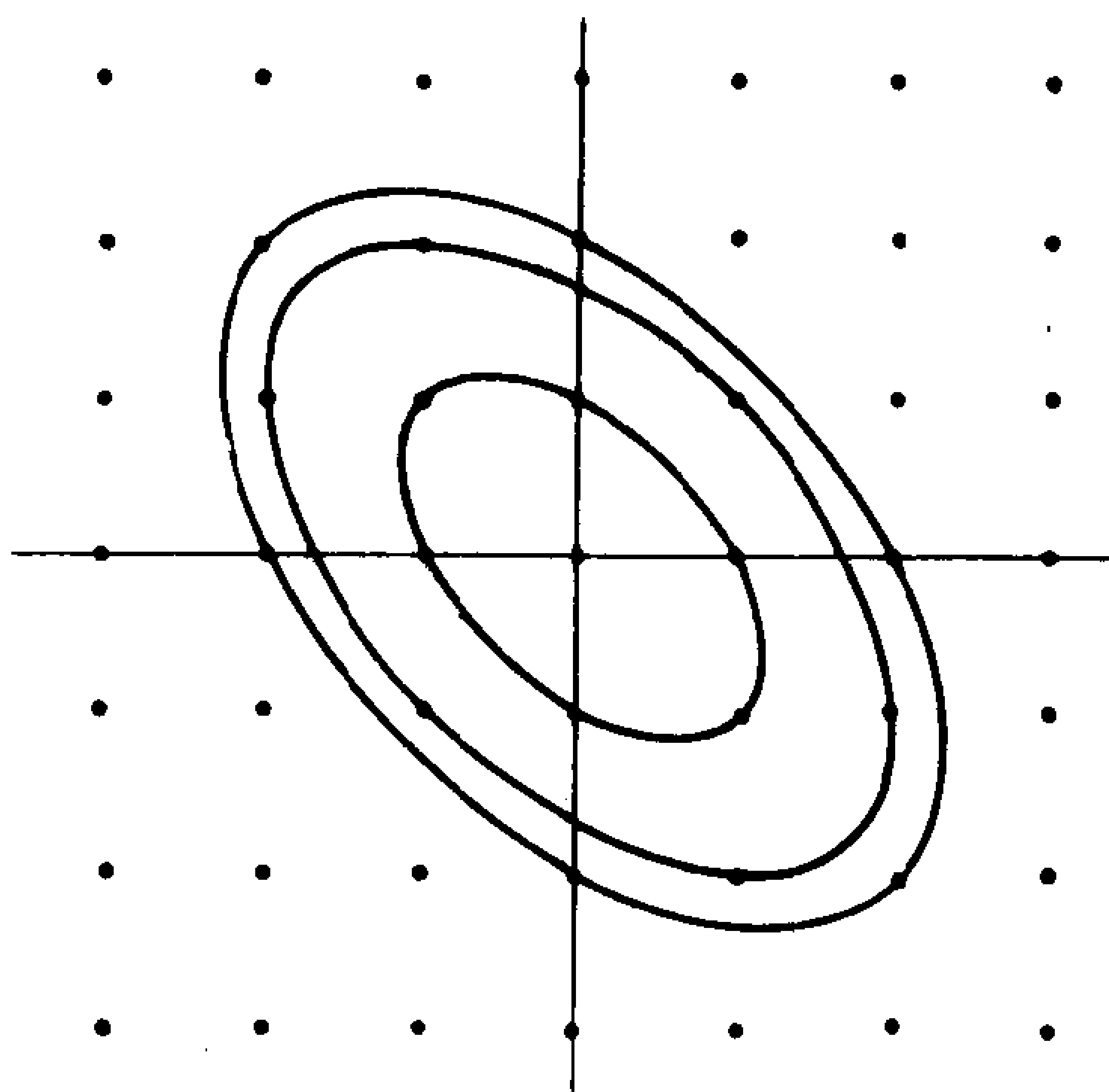
(iv) 同 (i).

(v) 自守变换群有十二个元素,与问题 75 中的群的同构.

77. $(MPM^{-1})^{\mathrm{T}}=M^{-1\mathrm{T}}P^{\mathrm{T}}M^{\mathrm{T}}$, 所以

$$(MPM^{-1})MAM^{\mathrm{T}}(MPM^{-1})^{\mathrm{T}}=MPAP^{\mathrm{T}}M^{\mathrm{T}},$$

当且仅当 $PAP^{\mathrm{T}}=A$ 时,它才等于 MAM^{T}.



$x^2+xy+y^2=1,3,4$ 的图形

图 8.4

这样，在型 $(x\ \ y)A\binom{x}{y}$和它的等价型 $(x\ \ y)MAM^{T}\binom{x}{y}$的自守变换之间有一个一一对应 $P\to MPM^{-1}$，这个对应是一个同构.

因为每个正定二次型等价于一个约化型，而在问题 76 中对约化型做了完整分类，所以这里所得到的自守变换群的分类也是完整的.

历 史 注 记

1816 年，J. Farey 与 A. L. Cauchy 证明了问题 14 的结果.

L. Euler 在 1761 年和 1763 年分别对二次型 x^2+3y^2 与 x^2+2y^2 做了详细研究. 1773 年，J. L. Lagrange 利用我们在问题 25 中所采用的等价概念证明：每个正定二次型等价于一个约化型，以及判别式为给定值的约化型是有限多个. 他还证明了我们关于正规

表示的定理 (问题 49 和问题 50). 1798 年, A. M. Legendre 证明, 不同的约化型不能等价. 1801 年, C. F. Gauss 将这个理论做了改进和推广, 并将正规等价与非正规等价加以区别(在替换 $(x, y) \to (px+ry, qx+sy)$ 下等价的两个二次型, 当 $ps-qr=1$ 时称为正规等价, 当 $ps-qr=-1$ 时称为非正规等价). Gauss 确定了在正规等价下的所有自守变换. 这个课题的详细历史, 见 Dickson 的书 (1950), 第三卷第一章.

第九章　数的几何

正方形格的子群

1．图9.1中，在正方形格上面放一个长方形格．取这两个格的一个公共点为原点，并按通常方式，用 $\mathbf{Z}\times\mathbf{Z}=\mathbf{Z}^2$ 中的元素标出正方形格的点．写出表示长方形格点的 $\mathbf{Z}^2$ 中的元素；再假定这个长方形格无限地延伸，证明它的全体格点对于矢量加法构成 $\mathbf{Z}^2$ 的子群．写出这个子群的两个生成元．

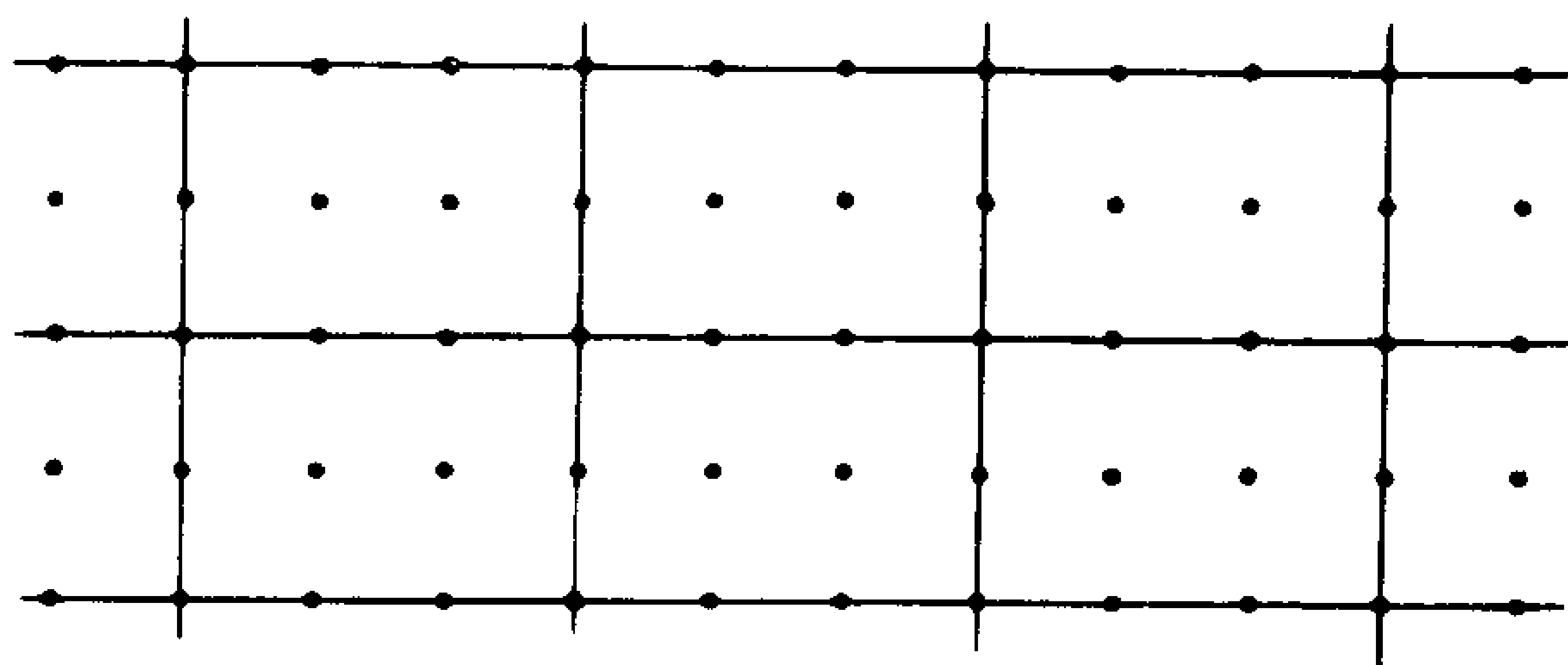


图 9.1

在本章中，总假定已经用 $\mathbf{Z}^2$ 的元素标出了在底下的正方形格①，并且把所研究的几个这样的格的一个公共点取为原点．

2．在图9.2中，求放在 $\mathbf{Z}^2$ 上的平行四边形格的点的坐标，证明这些点在矢量加法下构成 $\mathbf{Z}^2$ 的一个子群．求此子群的两个生成元．

① 在本章中，把集合 $\mathbf{Z}^2$ 和正方形格，以及 $\mathbf{Z}^2$ 的子群和相应的平行四边形格，都看做是同一的．——译者注

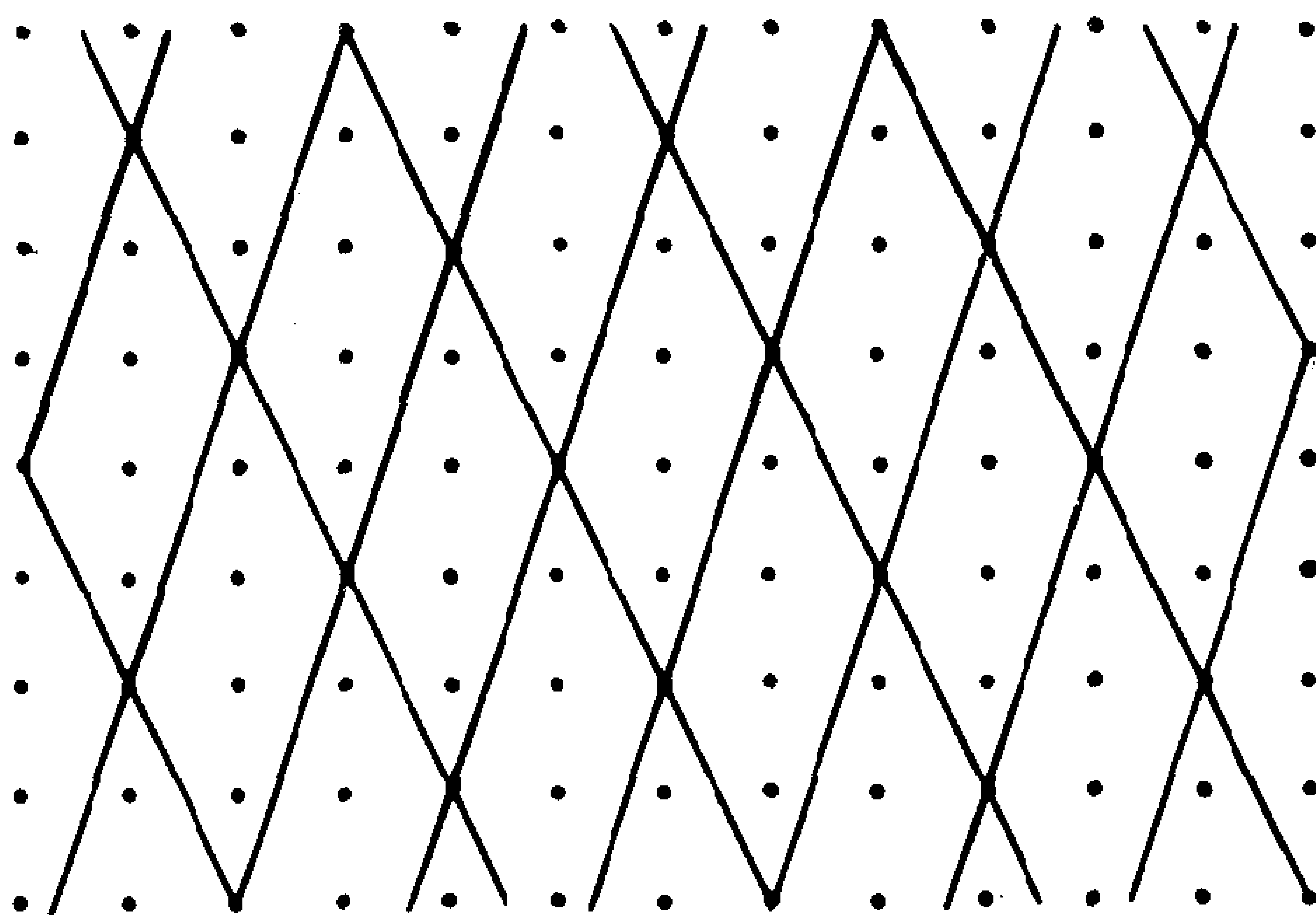


图 9.2

3. 在图 9.3 中，求放在 Z^3 上的平行四边形格的坐标，证明这些点在矢量加法下构成 Z^2 的一个子群，求这个子群的两个生成元.

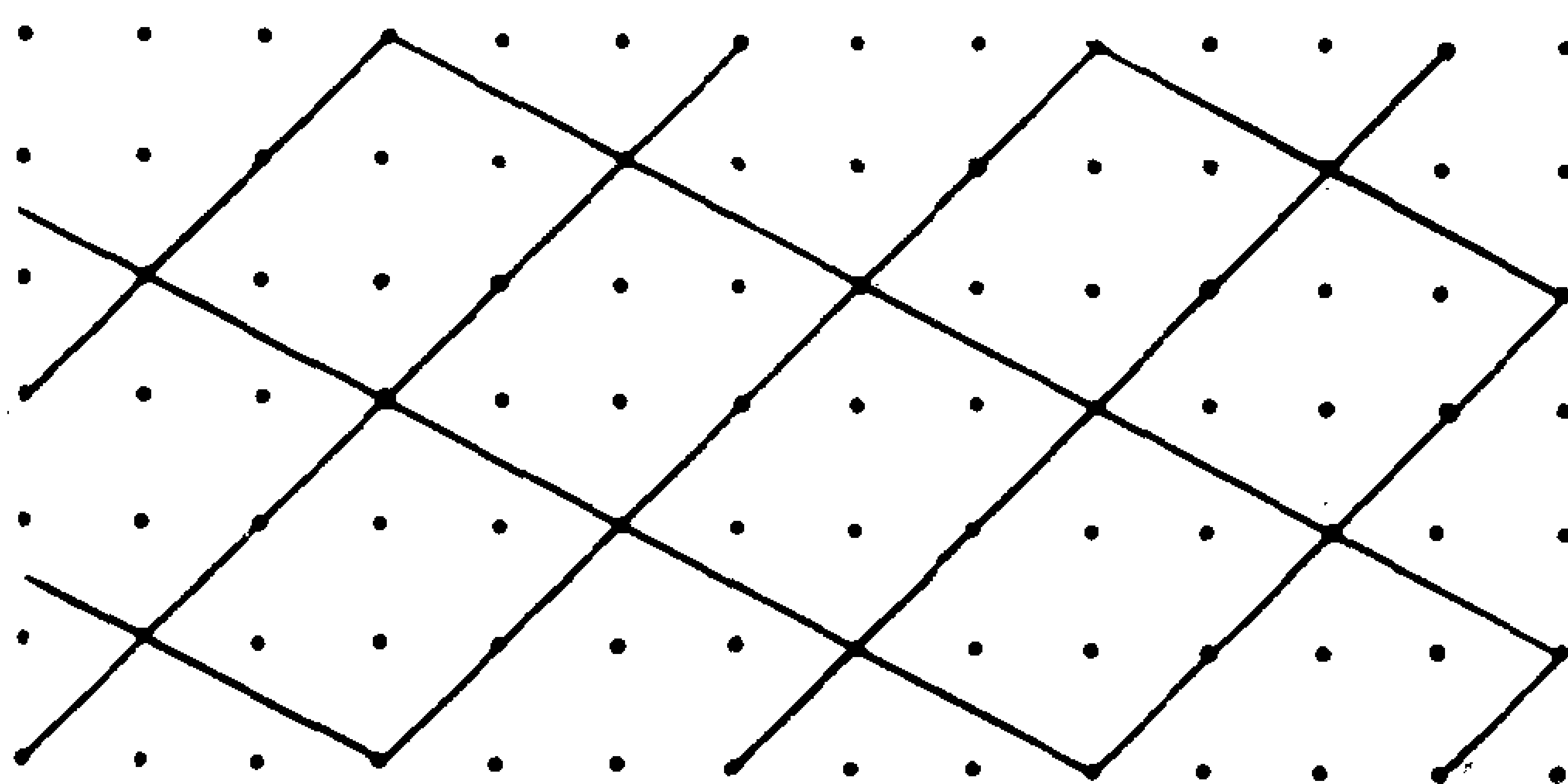


图 9.3

4. 证明：由 Z^2 的点所构成的任何平行四边形是 Z^2 的子群，此处假定这两个格的原点是同一个.

5．若 A，B 是 $\mathbf{Z}^2$ 中的点，不与原点 O 共线，则点 O，A，B，$A+B$ 是一个平行四边形的四个顶点，这个平行四边形称为子群 $<A,B>$ 的基本平行四边形．求问题1—3中每个子群的基本平行四边形的面积．

6．确定问题1—3中的子群的陪集．

7．τ：$(x,y)\to(x,y)+(a,b)$ 是格 $\mathbf{Z}^2$ 的一个平移，其中 $(a,b)\in\mathbf{Z}^2$．设 G 是 $\mathbf{Z}^2$ 的一个子群，它构成一个平行四边形格．当 $(a,b)\in G$ 时，称 τ 是 G 的一个平移．

确定下面给出的格点在 G 的平移之下所有可能的像：

(i) 给定的格点在 G 内．

(ii) 给定的格点不在 G 内．

8．设 O，A，B，$A+B$ 是群 $<A,B>$ 的一个基本平行四边形的顶点，证明：$\mathbf{Z}^2$ 的每一个点，都与基本平行四边形内部或边上的某个格点属于 $<A,B>$ 的同一个陪集．

9．由 $(6,0)$ 和 $(21,0)$ 所生成的 $\mathbf{Z}^2$ 的子群是什么？

10．由 $(20,10)$ 和 $(30,15)$ 所生成的 $\mathbf{Z}^2$ 的子群是什么？

11．设 $\mathbf{Z}^2$ 的一个子群是循环群，相应格点的几何排列是什么样子？

12．在什么条件下，由 (a,b) 和 (c,d) 生成的 $\mathbf{Z}^2$ 的子群是循环群？

13．求 $\mathbf{Z}^2$ 的两个元素，它们所生成的子群与 $(2,0)$，$(4,4)$ 和 $(5,2)$ 所生成的相同．

14．设 G 是 $\mathbf{Z}^2$ 的子群，(a,b) 和 (c,d) 是属于 G 且不与 $(0,0)$ 共线的元素，而且在 G 的所有这样的元素中，这两个点到 $(0,0)$ 的距离最小．证明：由 (a,b) 和 (c,d) 所生成的群是 G 的子群，而且，若 G 有元素不在 $<(a,b),(c,d)>$ 内，则会出现关于 G 中的元素到 $(0,0)$ 的距离最小的假设相矛盾的结果．

15．将 $\mathbf{Z}^2$ 的所有可能的子群按几何形状分类．

16．以 Π 表示由基本平行四边形 O，A，B，$A+B$ 的内部区

域及其除线段 $[A, A+B]$ 与 $[B, A+B]$ 外的边界所组成的区域. 在格 $<A, B>$ 的所有平移之下, Π 的像的并集是什么? 其中能有两个像相交吗?

17. 参看问题 8, 证明 $<A, B>$ 在 $\mathbf{Z}^2$ 中的陪集的个数等于 $\mathbf{Z}^2$ 在 Π 中的格点数. Π 的定义见问题 16.

18. 利用坐标求出图9.4 中在一个正方形格上画出的三个平行四边形的面积, 这里取小正方形作为面积单位. 能否找出平行四边形的面积与它的半闭区域 (定义见问题 16) 中的格点数目之间的关系?

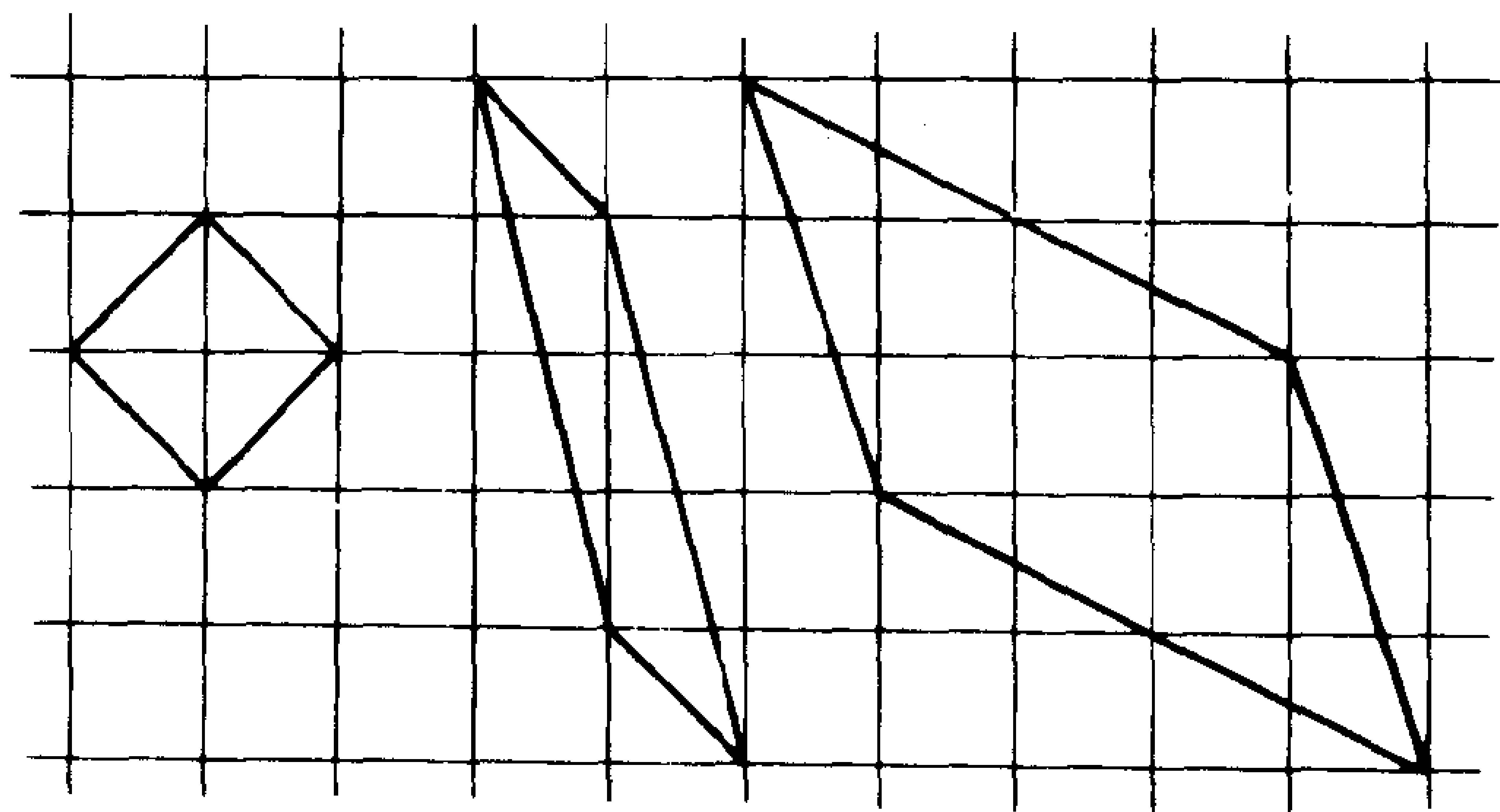


图 9.4

19. 对于图 9.1 — 9.3 中的每一个格, 各选一个基本平行四边形, 把左下方顶点落在基本平行四边形[1]中的那些单位正方形涂上色. 试比较涂色的单位正方形的总面积与区域的面积.

20. 在图 9.5 — 9.7 的每一个格中, 选定了基本平行四边形, 并且标出了最小顶点在它的区域中的那些单位正方形. 用几体方法说明为什么这些正方形面积之和等于平行四边形的面积 (正方

---

① 基本平行四边形的定义按问题 16 来理解, 下同—— 译者注.

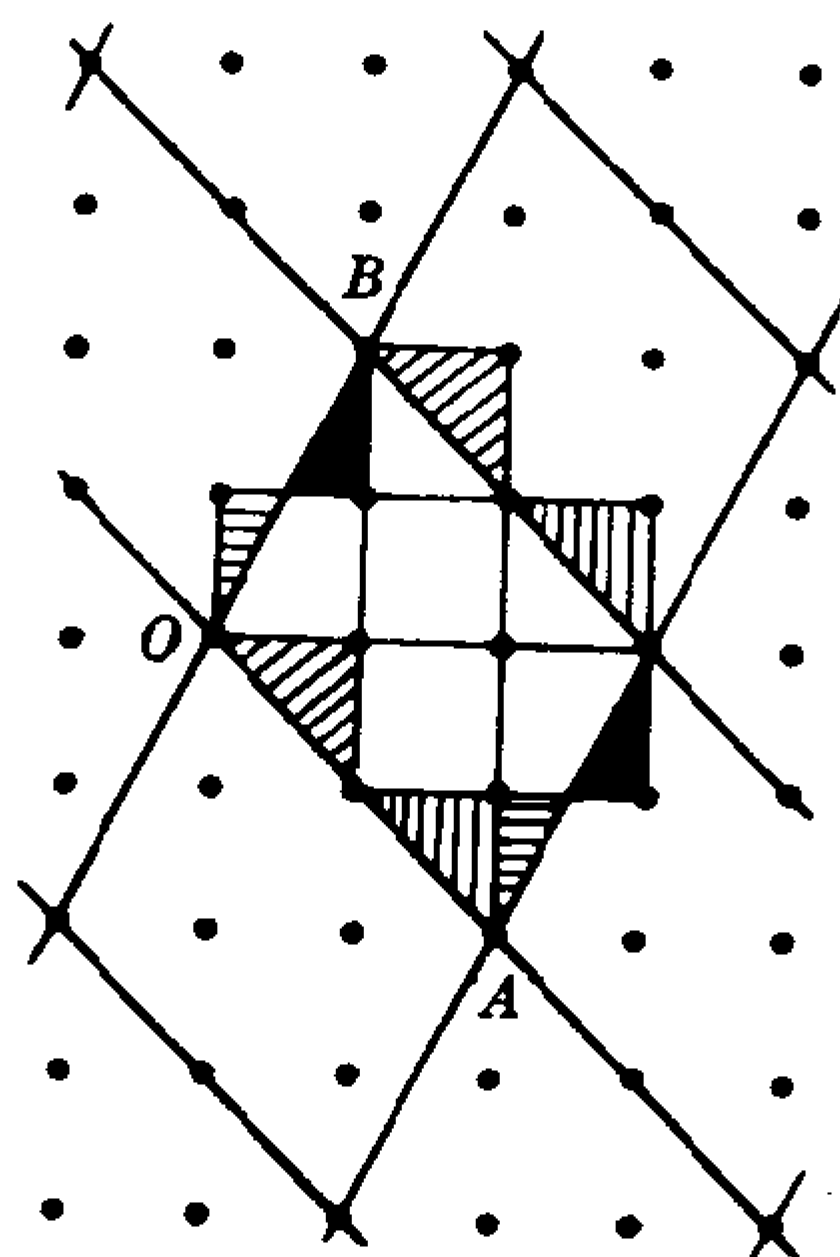


图 9.5

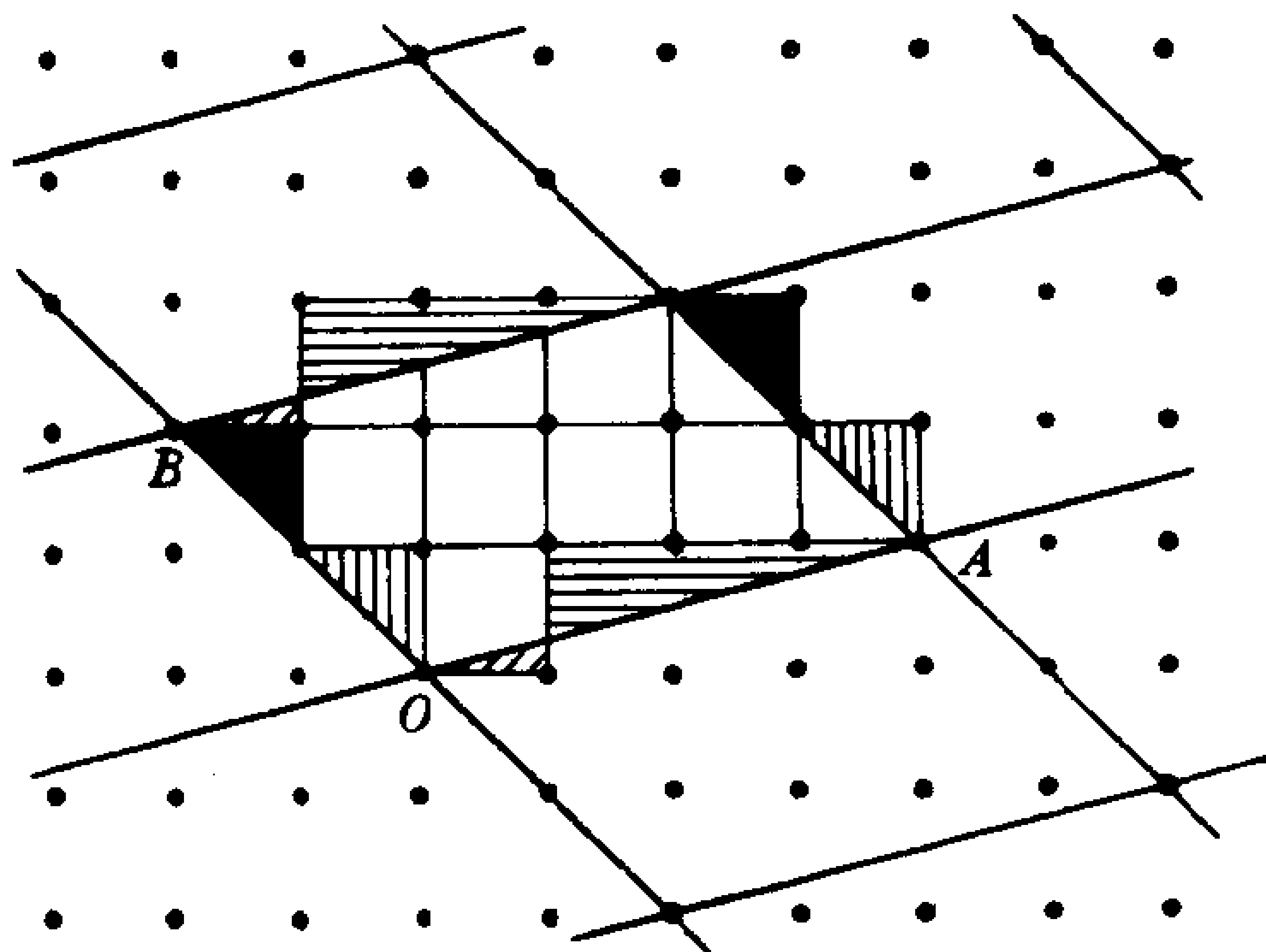


图9.6

形的最小顶点是指两个坐标都最小的顶点. 由于正方形的边与坐标轴平行,这个定义是明确的.)

21. 设 O,A,B 是 $\mathbf{Z}_2$ 中不共线的点. 按问题16 定义Π,并把最小顶点落在 Π 中的正方形的并集记为 Σ. 为了避免这些正方形相交,我们把每个正方形中的 x 坐标与y 坐标都是最大值的顶点所在的两条边去掉.

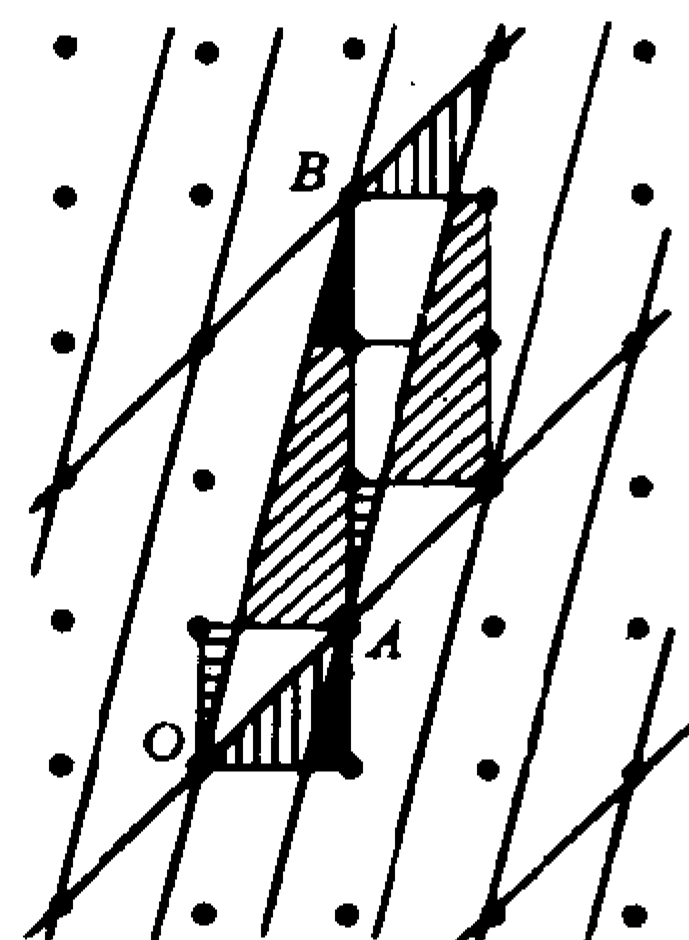


图 9.7

在格 $<A,B>$ 的平移之下,Σ 的任意两个像是否相交?

平面 $\mathbf{R}^2$的每一个点是否属于Σ在这个格的某个平移之下的像?

22. 用上题的记号,设 τ 是 $<A,B>$ 的一个平移. 为什么平面区域

$$\tau(\Pi)\cap\Sigma \quad 与 \quad \Pi\cap\tau^{-1}(\Sigma)$$

全等，因而面积相同？

对于所有可能的平移 τ，所有形如 $\tau(\Pi)\cap\Sigma$ 的区域的并集为什么就是区域 Σ？

对于所有可能的平移 τ，所有形如 $\Pi\cap\tau^{-1}(\Sigma)$ 的区域的并集为什么就是区域 Π？

证明 Π 与 Σ 有相同的面积．

23．证明平行四边形 $O,A,B,A+B$ 的面积等于 $<A,B>$ 在 $\mathbf{Z}^2$ 中的陪集个数．(这个重要定理还没有统一的名称)．

24．格 $<P,Q>$ 的任何两个(形状可能不同的)基本平行四边形的面积是否一定相同？

25．证明集合 $\{(x,y)\mid x+2y\equiv 0 \pmod 5\}$ 是 $\mathbf{Z}^2$ 的子群．从数值方面考虑，确定其陪集个数．在一个正方形格上画出这个子群．找出一个基本平行四边形，并求出它所含的格点数，以验证你的答案．

26．证明集合 $\{(x,y)\mid ax+by\equiv 0 \pmod n\}$ 是 $\mathbf{Z}^2$ 的子群．

27．$\mathbf{Z}^2$ 的下述子集各有多少陪集：

(i) $\{(x,y)\mid x+2y\equiv 0 \pmod{10}\}$，

(ii) $\{(x,y)\mid 2x+5y\equiv 0 \pmod{10}\}$，

(iii) $\{(x,y)\mid 2x+6y\equiv 0 \pmod{10}\}$？

对每一种情况，通过确定一个面积等于陪集个数的基本平行四边形，来证明每个子群构成一个平行四边形格．

28．利用孙子定理(问题 2.18)求 $\mathbf{Z}^2$ 的子群

$$\{(x,y)\mid x+y\equiv 0 \pmod 3\}\bigcap\{(x,y)\mid x+2y\equiv 0 \pmod 5\}$$

的基本平行四边形面积．

二维的 Minkowski 定理

首先，我们给出定理中用到的开、凸和对称的概念．

29. 平面上的开域是指这样的一个区域，它含有它的每个点的一个圆邻域．一个点的圆邻域是指以此点为圆心的一个圆的内部区域．

平面的下列子集中，哪些是开域：

(i) 一个点，

(ii) 一条线段，

(iii) 圆的内部区域，不包括圆周，

(iv) 圆的内部区域以及圆周，

(v) 区域 $\{(x,y)\mid -1<x<1\}$，

(vi) 区域 $\{(x,y)\mid -1\leqslant x\leqslant 1\}$，

(vii) 区域 $\{(x,y)\mid -\frac{1}{2}<x<\frac{1}{2}, -\frac{1}{2}<y<\frac{1}{2}\}$？

30. 设 R 是平面上的开域，面积为 Δ，含有格点 $(0,0)$，且落在正方形 $\{(x,y)\mid -r<x<r, -r<y<r\}$ 内．在整格 $\mathbf{Z}^2$ 的平移 $(x,y)\to(x,y)+(a,b)$（它将 $(0,0)$ 映射到 (a,b)）下，R 的像用 $R_{(a,b)}$ 表示．此外假设 $R_{(a,b)}$ 与 $R_{(c,d)}$ 没有公共点，除非 $(a,b)=(c,d)$．

(i) 求一个包含九个区域 $R_{(a,b)}$ $(a,b=0,1,-1)$ 的正方形．

(ii) 求一个包含二十五个区域 $R_{(a,b)}$ $(a,b=0,\pm1,\pm2)$ 的正方形．

(iii) 求一个包含 $(2n+1)^2$ 个区域 $R_{(a,b)}$ $(a,b=0,\pm1,\cdots,\pm n)$ 的正方形．

(iv) 证明 $\Delta\leqslant 4r^2$．

(v) 证明 $9\Delta\leqslant(2+2r)^2$．

(vi) 证明 $25\Delta\leqslant(4+2r)^2$．

(vii) 证明对任意的正整数 n，$(2n+1)^2\Delta\leqslant(2n+2r)^2$．

(viii) 证明对任意的正整数 n，

$$\Delta\leqslant\left(1+\frac{r-\frac{1}{2}}{n+\frac{1}{2}}\right)^2$$

(ix) 证明$\Delta \leqslant 1$.

(x) 举出一个区域 R,它满足问题中的条件,而且$\Delta = 1$.

以下四个问题涉及在线性变换之下内点的像.

31. 设$0<k<1$,a和c是实数,证明$ka+(1-k)c$在a与c之间.

32. 对任意实数k,证明点$(ak+(1-k)c, bk+(1-k)d)$与(a,b),(c,d)共线.

33. 利用问题31与问题32证明:

$$\{k(a,b)+(1-k)(c,d) \mid 0 \leqslant k \leqslant 1\}$$

是连结(a,b)与(c,d)的线段.

34. 假设在平面$\mathbf{R}^2$的线性变换下,$A \to A'$, $B \to B'$,证明线段$[A,B]$被映射成线段$[A',B']$.

再证明:在平面$\mathbf{R}^2$的线性变换下,若三角形ABC的像是三角形$A'B'C'$,则在这个变换下ABC的内部区域被映射成$A'B'C'$的内部区域.

35. 一个区域若含有连结它的任何两个点的线段,则称为凸域.下面的集合中,哪些是凸的:

(i) 一个点,

(ii) 一条线段,

(iii) 半圆的内部,

(iv) 半圆的内部及其边界,

(v) 半圆的边界,

(vi) 月牙状圆形的内部?

36. 一个平面区域,如果它的任何一点A在对点O做半周旋转后的像仍在这个区域内,则称它对点O对称.

是否存在一点,使

(i) 一个圆,

(ii) 一个长方形,

(iii) 一个等边三角形，

(iv) 两条平行直线间的无限带形，

对它是对称的？

37．举出英文字母为例，使得它

(i) 是凸的且对某一点对称，

(ii) 是凸的但对任何点都不对称，

(iii) 对某一点对称但不是凸的，

(iv) 不是凸的且对任何点都不对称．

38．设 R 是对点 O 对称的平面凸区域，τ 是将 O 变到 A 的平面平移，R_A 是 R 在平移 τ 下的像．设 R 与 R_A 相交且 $P\in R\cap R_A$，证明 $\tau^{-1}(P)\in R$．设 Q 是 $\tau^{-1}(P)$ 在对 O 做半周旋转下的像．通过考察以 P，$\tau^{-1}(P)$，Q，$\tau(Q)$ 为顶点的平行四边形，证明 OA 的中点属于 R．设 $2R$ 是区域 R 以 O 为中心放大二倍后的像，证明 $2R$ 包含 A．

39．设 R 是对 $(0,0)$ 对称的凸区域且面积大于 4．设 $\frac{1}{2}R$ 是 R 以 $(0,0)$ 为中心缩小 $\frac{1}{2}$ 后的像．证明：

(i) 对于整格 $\mathbf{Z}^2$ 的某个平移 τ，$\frac{1}{2}R$ 与 $\tau(\frac{1}{2}R)$ 相交（利用问题 30）．

(ii) $\frac{1}{2}R$ 含有从 $(0,0)$ 到 $\tau(0,0)$ 的线段的中点（利用问题 38）．

(iii) R 含有 $\mathbf{Z}^2$ 中与 $(0,0)$ 不同的格点．

(Minkowski 定理)．

下面的两个问题是二维 Minkowski 定理的简单但有用的推广．

40．考虑平面上的任一个平行四边形格，它的每一个基本平

行四边形的面积是 A .将一个基本平行四边形的顶点标为 $(0,0)$, $(1,0)$, $(1,1)$, $(0,1)$,进而按照通常定义的矢量加法标出所有的格点.设 R 是含有点 $(0,0)$的面积为 Δ 的开域,而且它整个地包含在以 $x=\pm r$, $y=\pm r$ 为边的平行四边形中,它在把 $(0,0)$变到 (a,b)的平行四边行格的平移下的像是 $R_{(a,b)}$. 又设 $R_{(a,b)}$ 与 $R_{(c,d)}$不相交,除非 $(a,b)=(c,d)$.证明

(i) $\Delta \leqslant (2r)^2 A$,

(ii) $9\Delta \leqslant (2+2r)^2 A$,

(iii) $25\Delta \leqslant (4+2r)^2 A$,

(iv) 对一切正整数 n , $(2n+1)^2\Delta \leqslant (2n+2r)^2 A$,

(v) $\Delta \leqslant A\left(1+\dfrac{r-\frac{1}{2}}{n+\frac{1}{2}}\right)^2$;

进而推出 $\Delta \leqslant A$.

41 . 对于基本平行四边形面积为 A 的任何平行四边形格,证明:对某个格点对称且面积大于 $4A$ 的凸域至少含有两个格点.

下面的五个问题,利用 Minkowski 定理给出了关于用特殊的二次型表示数的一些结果的不同的证明.

42 . 在通常的正方形格上,确定格

$$L=\{(x,y) \mid x-12y \equiv 0 \pmod{29}\}$$

的基本平行四边形的面积.

已知 $12^2 \equiv -1 \pmod{29}$,证明对于格 L 的每一点,有 $x^2+y^2 \equiv 0 \pmod{29}$.

证明在圆 $x^2+y^2=\dfrac{4}{3}\cdot 29$ 内除原点外还含有 L 中的一个点.

证明存在整数 x , y ,使得 $x^2+y^2=29$.

43 . 设 p 是素数且 $u \not\equiv 0 \pmod{p}$,求格

$$L=\{(x,y) \mid x-yu \equiv 0 \pmod{p}\}$$

的基本平行四边形的面积.

若 $p\equiv 1\pmod 4$且 $u^2\equiv -1\pmod p$,证明对于 L 中的每一点,有 $x^2+y^2\equiv 0\pmod p$.

证明在圆 $x^2+y^2=\frac{4}{3}p$ 内除点 $(0,0)$外还含有 L 中的一个点.

证明存在整数 x,y,使得 $x^2+y^2=p$.

44. 设 a 与 b 都不等于零,证明线性变换

$$(x,y)\to(x,y)\begin{pmatrix} a & 0\\ 0 & b\end{pmatrix}$$

将圆 $x^2+y^2=1$ 映成椭圆 $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$.证明这个椭圆的面积是 πab.

45. 在通常的正方形格上,求格

$$L=\{(x,y)|x-7y\equiv 0\pmod{17}\}$$

的基本平行四边形的面积.

已知 $7^2\equiv -2\pmod{17}$,证明$x^2+2y^2\equiv 0\pmod{17}$对于$L$ 的每个点成立.

证明在椭圆 $x^2+2y^2=(\frac{4}{3}\sqrt{2})17$ 内,除原点外,还含有 L 的一个点.进而推出,存在整数 x,y,使得 $x^2+2y^2=17$.

46. 利用问题4.42,验证:当$p\equiv 1,3\pmod 8$时有 $(\frac{-2}{p})=1$.

若$p\equiv 1,3\pmod 8$且 $u^2\equiv -2\pmod p$,证明格

$$\{(x,y)\mid x-uy\equiv 0\pmod p\}$$

中的每一个点都满足 $x^2+2y^2\equiv 0\pmod p$.

证明在椭圆 $x^2+2y^2=(\frac{4}{3}\sqrt{2})p$ 内,除原点外,至少还含有这个格的一个点,进而推出,存在整数 x,y,使得 $x^2+2y^2=p$.

由此至本章结束,全部问题的目的是为了将问题1 — 46的结果推广到三维的情形.

立方体格的子群

47. 证明 $\mathbf{Z}\times\mathbf{Z}\times\mathbf{Z}$[1]的子集

$$\{(x,y,z)\mid x\equiv 0\pmod 2\},$$

$$\{(x,y,z)\mid y\equiv 0\pmod 3\},$$

以及

$$\{(x,y,z)\mid z\equiv 0\pmod 5)$$

都是 $\mathbf{Z}^3$ 的在矢量加法下的子群.

这些子群各有多少陪集?

48. 证明 $\{(x,y,z)\mid 15x+10y+6z\equiv 0\pmod{30}\}$是问题47中 $\mathbf{Z}^3$ 的三个子群的交集.求这个子群的指数.

若按通常方法用 $\mathbf{Z}^3$ 的元素来标出立方体格的点,试确定这个子群所对应的格的基本平行六面体.

下面的两个问题给出了平行六面体的体积公式.讨论三维的幺模变换以及求 $\mathbf{Z}^3$ 的子群的指数时,都要用到这一公式.

49. 设 $O=(0,0,0)$,$A=(1,2,2)$以及 $B=(0,3,4)$是立方体格的点,求 OA,OB 及 AB 的长,并证明角 AOB 的余弦是 $\frac{14}{15}$.由此证明三角形 OAB 的面积是 $\frac{1}{2}\sqrt{29}$.

50. 设 $O=(0,0,0)$,$A=(a_1,a_2,a_3)$,$B=(b_1,b_2,b_3)$

[1] 设 $x,y,z\in\mathbf{Z}$,$\mathbf{Z}^3=\mathbf{Z}\times\mathbf{Z}\times\mathbf{Z}$ 是所有的点(x,y,z)组成的集合.—— 译者注.

以及 $D=(a_1+b_1, a_2+b_2, a_3+b_3)$是立方体格的点，证明角 AOB 的余弦是

$$\frac{a_1b_1+a_2b_2+a_3b_3}{\sqrt{(a_1^2+a_2^2+a_3^2)(b_1^2+b_2^2+b_3^2)}},$$

由此推出平行四边形 $OADB$ 的面积是

$$\sqrt{(a_2b_3-a_3b_2)^2+(a_3b_1-a_1b_3)^2+(a_1b_2-a_2b_1)^2}.$$

记 $E=(a_2b_3-a_3b_2, a_3b_1-a_1b_3, a_1b_2-a_2b_1)$，利用你所得到的关于余弦的结果证明 OE 垂直于 OA 及 OB，由此推出：由点 $C=(c_1, c_2, c_3)$到平行四边形 $OADB$ 的垂直距离等于 OC 乘以角 COE 的余弦.

证明以 OA, OB, OC 为棱的平行六面体的体积等于

$$|c_1(a_2b_3-a_3b_2)+c_2(a_3b_1-a_1b_3)+c_3(a_1b_2-a_2b_1)|,$$

即是行列式

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$$

的绝对值.

51. 设线性变换

$$(x, y, z)\to(x, y, z)\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

将 $\mathbf{Z}^3$ 满射到自身. 通过考虑 $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$的像和原像，证明

(i) $a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3$ 都是整数，

(ii) 所给出的 3×3 矩阵的行列式 Δ 是非零整数，

(iii) $\frac{b_2c_3-b_3c_2}{\Delta}$, $\frac{c_2a_3-c_3a_2}{\Delta}$, $\frac{a_2b_3-a_3b_2}{\Delta}$,

$\frac{b_3c_1-b_1c_3}{\Delta}$, $\frac{c_3a_1-c_1a_3}{\Delta}$, $\frac{a_3b_1-a_1b_3}{\Delta}$,

$\frac{b_1c_2-b_2c_1}{\Delta}$, $\frac{c_1a_2-c_2a_1}{\Delta}$, $\frac{a_1b_2-a_2b_1}{\Delta}$

都是整数，以及

(iv) 假定

$$\begin{pmatrix} b_2c_3-b_3c_2 & c_2a_3-c_3a_2 & a_2b_3-a_3b_2 \\ b_3c_1-b_1c_3 & c_3a_1-c_1a_3 & a_3b_1-a_1b_3 \\ b_1c_2-b_2c_1 & c_1a_2-c_2a_1 & a_1b_2-a_2b_1 \end{pmatrix}$$

的行列式就是 Δ^2，证明 $\frac{1}{\Delta}$ 是整数，从而推出 $\Delta=\pm1$.

52. 设 A 是元素为整数的 3×3 矩阵，其行列式为 ±1，证明线性变换

$$(x,y,z)\to(x,y,z)A$$

把 $\mathbf{Z}^3$ 满射到 $\mathbf{Z}^3$. 这种矩阵称为幺模矩阵，这种变换称为幺模变换.

下面的十四个问题是研究 $\mathbf{Z}^3$ 的子群，特别是有限指数的子群.

53. 如果 $\mathbf{Z}^3$ 的一个子群的元素都在过原点的一个平面上，那么与它们相对应的点可能有怎样的几何排列？

54. 设三个点 A,B,C 不在过原点的平面上，且是 $\mathbf{Z}^3$的子群 G 中离原点距离最近的点，证明 $G=\langle A,B,C\rangle$.

55. 如果 $\mathbf{Z}^3$ 的某个子群不是全部地在过原点的平面上，那么它所对应的点有怎样的几何排列？

56. 在矢量加法下，求 $\mathbf{Z}^3$ 的下列每个子群的三个生成元：

(i) $\{(x,y,z) \mid x \equiv 0 \pmod 2\}$,

(ii) $\{(x,y,z) \mid y \equiv 0 \pmod 3\}$,

(iii) $\{(x,y,z) \mid z \equiv 0 \pmod 5\}$,

(iv) $\{(x,y,z) \mid x \equiv 0 \pmod 2$ 且 $y \equiv 0 \pmod 3\}$,

(v) $\{(x,y,z) \mid 3x+2y \equiv 0 \pmod 6\}$,

(vi) $\{(x,y,z) \mid x \equiv 0 \pmod 2, y \equiv 0 \pmod 3,$

$z \equiv 0 \pmod 5\}$,

(vii) $\{(x,y,z) \mid 15x+10y+6z \equiv 0 \pmod{30}\}$.

57. 若点 A,B,C 与原点 O 不共面，则以 $O,A,B,C,B+C,C+A,A+B,A+B+C$ 为顶点的平行六面体，称为 $\mathbf{Z}^3$ 的子群 $\langle A,B,C\rangle$ 的基本平行六面体．

求问题 56 中各个子群的基本平行六面体的体积．

58. 问题 56 中，$\mathbf{Z}^3$ 的那些子群各有多少陪集？

59. 设 G 是 $\mathbf{Z}^3$ 的子群，仿照问题 7 定义格 G 的一个平移．

60. 设 G 是 $\mathbf{Z}^3$ 的一个子群，且不是整个地在一个平面上，那么，$\mathbf{Z}^3$ 的每一个点，是否必与指定的 G 的基本平行六面体内的某个点落在 G 的同一个陪集内？

61. 以 Π 表示基本平行六面体 $O,A,B,C,B+C,C+A,A+B,A+B+C$ 的内部区域以及它的各个面和各条棱，但不包括下面的三个面以及这三个面的棱：

$A, A+B, A+B+C, C+A$,

$B, B+C, A+B+C, A+B$,

$C, C+A, A+B+C, B+C$,

那么在格 $\langle A,B,C\rangle$ 的所有平移之下，Π 的像的并集是什么？任意的两个像是否相交？

62. 对于问题 56 中的最后一个子群的基本平行六面体，计算 $\mathbf{Z}^3$ 在（问题 61 中定义的）Π 内的格点数．

63. 为什么格 $\langle A,B,C\rangle$ 在 $\mathbf{Z}^3$ 中的陪集个数等于（在问题

61 中定义的）Π 中的格点数？

64．设 O, A, B, C 是 $\mathbf{Z}^3$ 中不共面的点，Π 按问题 61 定义，并规定区域 V 是最小顶点在 Π 中的那些单位立方体的并集．立方体的最小顶点是指三个坐标都是最小的点，这个定义对于各条棱都平行于坐标轴的立方体来说是明确的．为了避免这些立方体相交，我们把分别有最大 x，最大 y 和最大 z 的那三个面从这些立方体的并集 V 中去掉．

在格 $<A, B, C>$ 的平移之下，V 的两个像能否相交？

空间 $\mathbf{R}^3$ 中的点，是否都落在 V 经过格的一个平移后的像中？

65．使用上题的记号，并设 τ 是格 $<A, B, C>$ 的一个平移．为什么空间区域 $\tau(\Pi) \cap V$ 与 $\Pi \cap \tau^{-1}(V)$ 全等，因而体积相同？

对于所有可能的 τ，全体形如 $\tau(\Pi) \cap V$ 的区域的并集为什么就是区域 V？

对于所有可能的 τ，全体形如 $\Pi \cap \tau^{-1}(V)$ 的区域的并集为什么就是区域 Π？

证明 Π 与 V 体积相同．

66．设 O, A, B, C 不共面，证明平行六面体 $O, A, B, C, B+C, C+A, A+B, A+B+C$ 的体积等于 $<A, B, C>$ 在 $\mathbf{Z}^3$ 中的陪集个数．(这个重要定理还没有统一的名称)．

三维的 Minkowski 定理

67．仿照问题 29，定义三维空间的开域．$\mathbf{R}^3$ 的下述子集中哪一些是开域：

(i) 一个点，

(ii) 一条线段，

(iii) 一个圆盘，

(iv) 一个球的内部，但不包括表面，

(v) 一个球的内部及表面，

(vi) 区域$\{(x,y,z) \mid -1<x<1\}$，

(vii) 区域$\{(x,y,z) \mid -1\leqslant x\leqslant 1\}$，

(viii) 区域$\{(x,y,z) \mid -\frac{1}{2}<x<\frac{1}{2},-\frac{1}{2}<y<\frac{1}{2},$

$-\frac{1}{2}<z<\frac{1}{2}\}$？

68．设开域 R 含有点 $(0,0,0)$，而且在 $\mathbf{Z}^3$ 的所有平移下，它的像都没有交点，试建立与问题 30 相类似的三维情形下的结论．

69．由 $(x,y,z)\to(-x,-y,-z)$ 所给出的空间映射称为关于 $(0,0,0)$ 的反演．一个区域称为对于点 O 在空间中对称，如果这个区域中的每一个点 A 在关于点 O 的反演下的像也属于这个区域．

给出 $\mathbf{R}^3$ 中体积不为零的下述各类型区域的例子：

(i) 是凸的且关于一个点是对称的，

(ii) 是凸的，但关于任意点都不对称，

(iii) 关于一个点对称，但不是凸的，

(iv) 既不是凸的，又关于任意点都不对称．

70．叙述并证明与问题 38 类似的关于三维情形下的结论．

71．叙述三维空间中与 Minkowski 定理(问题 39)类似的定理．

72．仿照问题 40 证明：设 R 是三维空间中的开区域，它含有点 $(0,0,0)$，而且对于 $\mathbf{Z}^3$ 中的任意一个给定的平行六面体格，在这个格的平移之下，R 的任何两个像都不相交，那么 R 的体积不大于基本平行六面体的体积．

73．仿照问题 41 证明：对于任何平行六面体格，若它的基本平行六面体的体积是 V，那么关于某个格点对称而且体积大于 $8V$ 的凸域中至少有两个格点．

关于 $ax^2+by^2+cz^2=0$ 的 Legendre 定理

现在，我们来详细地说明证明 Legendre 定理的技巧，这就是本章余下部分的内容。

74. 设 $y\equiv z \pmod 3$，证明 $15x^2+14y^2-71z^2\equiv 0 \pmod 3$。

设 $z\equiv 2y \pmod 5$，证明 $15x^2+14y^2-71z^2\equiv 0 \pmod 5$。

进而推出：若 $y\equiv z \pmod 3$ 且 $z\equiv 2y \pmod 5$，则

$$15x^2+14y^2-71y^2\equiv 0 \pmod{15}.$$

格

$$\{(x,y,z)\mid y\equiv z \pmod 3\}\cap\{(x,y,z)\mid z\equiv 2y \pmod 5\}$$

的基本平行六面体的体积是多少？

75. 设 $x\equiv z \pmod 7$，证明 $15x^2+14y^2-71z^2\equiv 0 \pmod 7$。

设 $y\equiv 2x \pmod{71}$，证明 $15x^2+14y^2-71z^2\equiv 0 \pmod{71}$。

进而推出：若 $x\equiv z \pmod 7$ 且 $y\equiv 2x \pmod{71}$，则

$$15x^2+14y^2-71z^2\equiv 0 \pmod{497}.$$

格

$$\{(x,y,z)\mid x\equiv z \pmod 7\}\cap\{(x,y,z)\mid y\equiv 2x \pmod{71}\}$$

的基本平行六面体的体积是多少？

76. 设 $x\equiv y \pmod 4$ 及 $y\equiv 0 \pmod 2$，证明

$$15x^2+14y^2-71z^2\equiv 0 \pmod 8.$$

77. 格

$\{(x,y,z)\mid y\equiv z \pmod 3,\ z\equiv 2y \pmod 5,\ x\equiv y \pmod 7,\ y\equiv 2x \pmod 7,\ x\equiv z \pmod 4,\ y\equiv 0 \pmod 2\}$ 的基本平行六面体的体积是多少？

证明这个格的点都满足

$15x^2+14y^2-71z^2\equiv 0 \pmod{4\cdot 15\cdot 14\cdot 71}$.

78. 设 $a,b,c\neq 0$，证明线性变换

$$(x,y,z)\to(x,y,z)\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$$

把球面 $x^2+y^2+z^2=1$ 映成椭球面 $\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1$. 证明这个椭球的体积是 $\frac{4}{3}\pi abc$.

79. 证明椭球

$$15x^2+14y^2+71z^2\leqslant 4\cdot 15\cdot 14\cdot 71$$

的体积是

$$\frac{4}{3}\pi\sqrt{4\cdot 14\cdot 71\cdot 4\cdot 15\cdot 71\cdot 4\cdot 15\cdot 14}$$

$$=\frac{4}{3}\pi\cdot 8\cdot 15\cdot 14\cdot 71>8\ (4\cdot 15\cdot 14\cdot 71).$$

80. 由问题 73 与问题 79 证明：在问题 77 的格中，存在异于原点的一个格点，它落在椭球 $15x^2+14y^2+71z^2=4\cdot 15\cdot 14\cdot 71$ 内部. 设这个格点是 (x_1,y_1,z_1)，证明

$$|15x_1^2+14y_1^2-71z_1^2|<4\cdot 15\cdot 14\cdot 71,$$

进而推出

$$15x_1^2+14y_1^2-71z_1^2=0.$$

81. 存在整数 x,y,z，使得

$$3x^2+5y^2-23z^2=0 \text{ 且 } \gcd(x,y,z)=1.$$

x,y,z 中可以有几个偶数，几个奇数？

82. 存在整数 x,y,z，使得

$$3x^2+5y^2-62z^2=0 \text{ 且 } \gcd(x,y,z)=1.$$

证明 x 与 y 必是奇数，由此推出 $x^2\equiv y^2\equiv 1 \pmod 8$. 并证

明 z 是偶数.此外,再证明 $x\equiv\pm y \pmod 4$.

83. 存在整数 x,y,z,使得

$$3x^2+7y^2-2z^2=0 \quad 且 \quad \gcd(x,y,z)=1.$$

证明 $x^2\equiv y^2\equiv 1 \pmod 8$. 由此推出 z 是奇数且 $x\equiv\pm y$ $\pmod 4$.

84. 设 x_1,y_1,z_1 是整数,使得

$$ax_1^2+by_1^2+cz_1^2=0 \pmod 8,$$
$$\gcd(ax_1,by_1,cz_1,4abc)=1,$$

其中 c 是偶数,证明

(i) ax_1 与 by_1 是奇数,

(ii) 若 z_1 是偶数,则 $a+b\equiv 0 \pmod 8$,

(iii) 若 z_1 是奇数,则 $a+b+c\equiv 0 \pmod 8$.

进而推出:若 $x\equiv y \pmod 4$且 $z\equiv z_1x \pmod 2$,则

$$ax^2+by^2+cz^2\equiv 0 \pmod 8.$$

85. 设整数 x_1,y_1,z_1 使得

$$ax_1^2+by_1^2+cz_1^2\equiv 0 \pmod p,$$

其中p 是整除 a 的奇素数,且

$$\gcd(ax_1,by_1,cz_1,4abc)=1,$$

指出如何求 l,使得当 $y\equiv lx \pmod p$时,

$$ax^2+by^2+cz^2\equiv 0 \pmod p$$

成立.

86. 设整数 x_1,y_1,z_1 使得

$$ax_1^2+by_1^2+cz_1^2\equiv 0 \pmod{4abc},$$

其中 a,b,c 都没有平方因子,两两互素,而且 $\gcd(ax_1,by_1,cz_1,$ $4abc)=1$.试构造一个格,其基本平行六面体的体积是 $|4abc|$,而且对于这个格的每个格点 (x,y,z),有

$$ax^2+by^2+cz^2\equiv 0 \pmod{4abc}.$$

求椭球

$$|a|x^2+|b|y^2+|c|z^2\leqslant 4|abc|$$

的体积，并且证明至少有一个异于原点的格点是在椭球内部．

证明

$$ax^2+by^2+cz^2=0$$

存在整数解．

(Legendre 定理)．

注记与答案

参考书见书目：Hardy 与 Wright (1980)，第三章．

1．$(3m, 2n)$．这个群由 $(3, 0)$ 和 $(0, 2)$ 生成．

2．根据矢量加法的平行四边形法则，对加法是封闭的．平行四边形格的每个元素都是 $m(1, -2)+n(1, 3)$ 的形式．

3．平行四边形格的每一个点都是 $m(2, -2)+n(2, 1)$ 的形式．

4．根据加法的平行四边形法则，是封闭的．因为它关于两个格的任一公共点是对称的，所以含有逆元素．

5．问题 1，6；问题 2，5；问题 3，6．

6．问题 1：$(3m, 2n)+(1, 0)$，

$(3m, 2n)+(2, 0)$，

$(3m, 2n)+(0, 1)$，

$(3m, 2n)+(1, 1)$，

$(3m, 2n)+(2, 1)$，

以及子群本身．

问题 2：$(m+n, -2m+3n)+(1, -1)$

$(m+n, -2m+3n)+(1, 0)$

$(m+n, -2m+3n)+(1, 1)$

$(m+n, -2m+3n)+(1, 2)$

以及子群本身．

问题 3： $(2m+2n, -2m+n)+(1, -1)$,

$(2m+2n, -2m+n)+(2, -1)$,

$(2m+2n, -2m+n)+(3, -1)$,

$(2m+2n, -2m+n)+(1, 0)$,

$(2m+2n, -2m+n)+(2, 0)$,

以及子群本身.

7. (i) G 的平移将 G 满射到 G.

(ii) 在 G 的所有平移之下,一个点的所有的像构成 G 在 $\mathbf{Z}^2$ 中的一个陪集.

8. $\mathbf{Z}^2$ 的每个格点都是在格 $<A, B>$ 的某个平行四边形的内部或边上;但这个平行四边形是平行四边形 $O, A, B, A+B$ 在 $<A, B>$ 的一个平移之下的像,所以原来的格点在 $O, A, B, A+B$ 中有一个原像,从而与它属于同一个陪集.

9. $(3n, 0)$.

10. $(10n, 5n)$.

11. 所有格点都在过原点的一条直线上.

12. $(0,0)$, (a,b), (c,d) 这三点共线.

13. 利用正方形格纸找出离 $(0,0)$ 最近的生成元. 点 $(2,0)$, $(1,2)$, $(-1,2)$ 中的任意两个.

14. 显然, (a,b) 和 (c,d) 生成一个平行四边形格. 若 G 有一点不在这个格上,那么由这个格的某个平移就得到 G 的一个点,它在三角形 $(0,0)$, (a,b), (c,d) 的内部,或是在三角形 $(0,0)$, $(-a,-b)$, $(-c,-d)$ 的内部. 在任何一种情况, G 都含有一个比 (a,b) 或 (c,d) 更靠近 $(0,0)$ 的点.

15. 或者是一个点,或者是共线的一些点(一个生成元),或者是一个平行四边形格(两个生成元).

16. 全平面. 若 Π 的两个像相交,则必重合.

17. 因为不存在将 Π 的一个格点映到另一个格点的 $<A, B>$ 的平移,所以 Π 的每个格点属于 $<A, B>$ 的不同陪集. 在

$<A, B>$ 的平移之下，$\mathbf{Z}^2$ 的每一个点都可以映射到 Π 中的一个格点，所以 $<A, B>$ 的每个陪集在 Π 中有一个代表元素.

18. 根据问题 8.5，这些面积分别等于矩阵

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix}$$

的行列式，即 2，3，10.

面积等于其中（按问题 16 的规定）的格点数目. Pick 定理（见 H.S.M.Coxeter，的书：*Introduction to geometry*，Wiley 1969）证明了这一联系，但我们在问题 19—23 中则给出了一个更一般的论证，它可推广到三维或高维的情形.

19. 在每一种情形，涂了色的单位正方形的面积之和等于平行四边形的面积.

20. 利用格的平移可以使得这些正方形在平行四边形外的互不相交部分与平行四边形的未被覆盖部分一一对应.

21. Σ 的任何两个不同的像不相交. 因为平面的每个点属于一个单位正方形，而每个单位正方形是 Σ 中某个单位正方形在格的平移之下的像，所以整个平面被 Σ 在格的所有平移之下的像所覆盖.

22. τ 将 $\Pi \cap \tau^{-1}(\Sigma)$ 满射到 $\tau(\Pi) \cap \Sigma$，所以这两个区域全等. $\tau(\Pi) \cap \Sigma$ 的点都在 Σ 内. 所有 $\tau(\Pi)$ 的集合覆盖全平面，因而所有 $\tau(\Pi) \cap \Sigma$ 的集合覆盖整个 Σ. $\Pi \cap \tau^{-1}(\Sigma)$ 的点都在 Π 内. 所有 $\tau^{-1}(\Sigma)$ 的集合覆盖全平面，因而所有 $\Pi \cap \tau^{-1}(\Sigma)$ 的集合覆盖整个 Π.

23. 陪集的个数 = 基本平行四边形中的格点数
= 最小顶点是这区域中格点的单位正方形个数
= 这些单位正方形的面积之和
= 平行四边形面积.

24．是的，因为陪集个数是子群的固有性质，而不是所选取的生成元的固有性质．

25．陪集是 $x+2y\equiv 0 \pmod 5$，

$x+2y\equiv 1 \pmod 5$，

$x+2y\equiv 2 \pmod 5$，

$x+2y\equiv 3 \pmod 5$，

以及 $x+2y\equiv 4 \pmod 5$．

26．若 $ax+by\equiv 0 \pmod n$ 且 $ax'+by'\equiv 0 \pmod n$，则 $a(x+x')+b(y+y')\equiv 0 \pmod n$，所以这个集合是封闭的．又因 $a(-x)+b(-y)\equiv 0 \pmod n$，所以它含有每个元素的逆元素．

27．(i) 10，例如 $(2,-1)$ 和 $(2,4)$．

(ii) 10，例如 $(5,0)$ 和 $(0,2)$．

(iii) 5，例如 $(2,1)$ 和 $(5,0)$．

28．因为 $\gcd(3,5)=1$，所以对于每个 x，存在唯一的 $y \pmod{15}$，使得

$$x+y\equiv 0 \pmod 3$$

且

$$x+2y\equiv 0 \pmod 5.$$

这个群，例如，可以是由 $(1,2)$ 和 $(-1,13)$ 生成；面积是15．

29．(iii)，(v)，(vii)．

30．(i) $|x|,|y|< r+1$．

(ii) $|x|,|y|< r+2$．

(iii) $|x|,|y|< r+n$．

(iv)—(vii) 区域面积不超过它所在的正方形面积．

(viii) 将 (vii) 中的不等式两边除以 $(2n+1)^2$ 可得到．

(ix) 在 (viii) 中令 $n\to\infty$．

(x) $|x|,|y|<\dfrac{1}{2}$．

31．设$a>c$，则 $a-c>0$．

由 $1>k>0$

得出 $a-c>k(a-c)>0$．

从而 $a>k(a-c)+c>c$．

或 $a>ka+(1-k)c>c$．

若$c>a$，则由$1>1-k>0$可以类似地证明．

32．$(ak+(1-k)c,bk+(1-k)d)$

$= (c,d)+k(a-c,b-d)$．

连结原点与$(a-c,b-d)$的线段平行于连结(a,b)与(c,d)的线段，所以所说的点落在过(c,d)与(a,b)的直线上．

33．由问题32知，这个集合中的每一个点都在连结(a,b)与(c,d)的直线上；由问题31知，每个点都在连结这两点的线段上，而且按$1-k:k$的比例把这两点分开．

34．设在平面的线性变换下，$(a,b)\to(a,b)'$，$(c,d)\to(c,d)'$，则

$$k(a,b)+(1-k)(c,d)\to k(a,b)'+(1-k)(c,d)',$$

所以，线段被映射成线段．因此，三角形的边被映射成三角形的边，而每个内点是在连结边上的两点的线段上．

35．除(v)与(vi)外都是．

36．(i)．(ii)：只有一个点；(iii)：这种点不存在；(iv)：有许多点．

37．(i)：O的内部．(ii)：D的内部．(iii)：H的全部线段．(iv)：L的全部线段．

38．$P\in R_A\Rightarrow\tau^{-1}(P)\in\tau^{-1}(R_A)=R$．

因为R关于O对称，所以$Q\in R$且$\tau(Q)\in R_A$．O是$\tau^{-1}(P)Q$中的点，而A是$P\tau(Q)$的中点，所以OA的中点是平行四边形的中心．但$P,Q\in R$，而且R是凸的，所以PQ的中点属于R，它也是OA的中点．

39. (i) 若$\frac{1}{2}R$不与任何一个$\tau(\frac{1}{2}R)$相交，则由问题30得到，$\frac{1}{2}R$的面积不大于1.

(ii) 因为$\frac{1}{2}R$与$\tau(\frac{1}{2}R)$相交，由问题38知道$(0,0)$与$\tau(0,0)$的中点在$\frac{1}{2}R$内.

(iii) 因此$\tau(0,0)$属于R.

40. 证明与问题30的证明是类似的.

41. 设R是关于一个格点对称且面积大于$4A$的凸区域.这时$\frac{1}{2}R$的面积大于A，所以，由问题40知道，它必与它自已在格的某个平移之下的像相交.由问题38的论证知道，连结$\frac{1}{2}R$的中心与它在这个格平移下的像的中心的线段的中点属于$\frac{1}{2}R$.因此，R含有它自已在格的这个平移之下的像的中心.

42. 面积是29.

若$x\equiv 12y \pmod{29}$，则$x^2+y^2\equiv 12^2y^2+y^2\equiv 0 \pmod{29}$.圆$x^2+y^2=\frac{4}{3}\cdot 29$是凸的，关于$(0,0)$对称，并且面积是$\pi\cdot\frac{4}{3}$.$29>4\cdot 29$故由问题41知,它含有这个给定的格的异于$(0,0)$的点.设这点是$(a,b)$，则$a^2+b^2\equiv 0 \pmod{29}$，但是$a^2+b^2<\frac{4}{3}\cdot 29<2\cdot 29$，所以$a^2+b^2=29$.

43. 面积是p.

$$x^2+y^2\equiv y^2u^2+y^2\equiv y^2(u^2+1)\equiv 0 \pmod{p}.$$

圆$x^2+y^2\equiv\frac{4}{3}p$是凸的，关于$(0,0)$对称，它的面积为$\pi\cdot\frac{4}{3}p>4p$，故由问题41知，它含有这个给定的格的异于$(0,0)$

的点．设这点是 (a,b)，则 $a^2+b^2\equiv 0 \pmod p$，但 $a^2+b^2<\frac{4}{3}p$ $<2p$，所以 $a^2+b^2=p$．这是下述结论的另一个证明：每一个同余于 $1 \pmod 4$ 的素数 p 可表示为二平方之和，这个证明与第六章无关．

44．当且仅当 (ax,by) 在曲线 $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$ 上时，(x,y) 在曲线 $x^2+y^2=1$ 上．在平面的线性变换下，面积要乘以相应矩阵的行列式．见问题 8．3 与问题 8．5．

45．面积是 17．

$$x^2+2y^2\equiv 49y^2+2y^2\equiv 51y^2\equiv 0 \pmod{17}.$$

椭圆 $x^2+2y^2\equiv(\frac{4}{3}\sqrt{2})\cdot 17$ 是凸的且关于 $(0,0)$ 对称，它的面积是 $\pi\cdot\frac{4}{3}\cdot 17>4\cdot 17$．所以，由问题 41 知，它含有这个给定的格的异于 $(0,0)$ 的点．设这个点是 (a,b)，则 $a^2+2b^2\equiv 0 \pmod{17}$，但 $a^2+2b^2<(\frac{4}{3}\sqrt{2})\cdot 17<2\cdot 17$，所以 $a^2+2b^2=17$．

46．面积是 p．

$$x^2+2y^2\equiv u^2y^2+2y^2\equiv(u^2+2)y^2\equiv 0 \pmod p.$$

这个椭圆是凸的，中心在原点，面积为 $\pi\cdot\frac{4}{3}p>4p$．由问题 41 知，它含有这个给定的格的异于 $(0,0)$ 的点．设此点为 (a,b)，则 $a^2+2b^2\equiv 0 \pmod p$，但 $a^2+2b^2<(\frac{4}{3}\sqrt{2})p<2p$，所以

$$a^2+2b^2=p.$$

47．每个集合都是封闭的，并且含有　元素的逆元素．

陪集个数分别为 2，3，5.

48. $x\equiv 0 \pmod 2$ 及 $y\equiv 0 \pmod 3 \Longleftrightarrow 3x+2y\equiv 0 \pmod 6$；$3x+2y\equiv 0 \pmod 6$ 及 $z\equiv 0 \pmod 5 \Longleftrightarrow 5(3x+2y)+6z\equiv 0 \pmod{30}$. 这个子群有 30 个陪集. 以平面 $x=0$，2；$y=0$，3；$z=0$，5 为界的长方体.

49. $OA=\sqrt{1^2+2^2+2^2}=3$，

$OB=\sqrt{0^2+3^2+4^2}=5$，

$AB=\sqrt{1^2+(3-2)^2+(4-2)^2}=\sqrt{6}$，

$AB^2=OA^2+OB^2-2\cdot OA\cdot OB\cdot\cos AOB$，

所以

$$6=9+25-2\cdot 5\cdot 3\cdot\cos AOB,\quad \cos AOB=\frac{14}{15}.$$

三角形 AOB 的面积 $=\frac{1}{2}OA\cdot OB\cdot\sin AOB$

$$=\frac{1}{2}\cdot 3\cdot 5\cdot\sqrt{1-\left(\frac{14}{15}\right)^2}$$

$$=\frac{1}{2}\sqrt{225-196}=\frac{1}{2}\sqrt{29}$$

50. 由余弦公式，$\cos AOB=\dfrac{OA^2+OB^2-AB^2}{2\cdot OA\cdot OB}$.

平行四边形面积 $=OA\cdot OB\cdot\sin AOB$.

当 $\cos AOB=0$ 或 $a_1b_1+a_2b_2+a_3b_3=0$ 时，OA 垂直于 OB.

平行六面体体积 $=OADB$ 的面积 $\cdot C$ 到这个平面的垂直距离.

51. (i) $(1,0,0)$的像是 (a_1,a_2,a_3)，等等，所以矩阵的元素都是整数.

(ii) 由 (i)知道 Δ 是整数. 若 $\Delta=0$，则 (a_1,a_2,a_3)，$(b_1,b_2$，

b_3)，(c_1，c_2，c_3)与原点共面，那么这个变换不能将 $\mathbf{Z}^3$ 满射到自身．

(iii) 此处的三个三元数组分别给出了映到 (1，0，0)，(0，1，0)，(0，0，1)的点的坐标．

(iv) 由 (1，0，0)，(0，1，0) 及 (0，0，1)的原像所构成的矩阵的行列式是 $\frac{\Delta^2}{\Delta^3}=\frac{1}{\Delta}$．因为这个矩阵的元素都是整数，所以 $\frac{1}{\Delta}$ 是整数．但若 Δ 与 $\frac{1}{\Delta}$ 都是整数，则必是 $\Delta=\pm 1$．

52．因为 A 的元素是整数，所以这个变换将 $\mathbf{Z}^3$ 内射到 $\mathbf{Z}^3$．因为 A 的行列式等于 ± 1，所以 (1，0，0)，(0，1，0)及 (0，0，1)的原像也是 $\mathbf{Z}^3$ 中的点．因此，$\mathbf{Z}^3$ 上的这个映射是一一对应的，且将 $\mathbf{Z}^3$ 满射到 $\mathbf{Z}^3$．

53．它们或者是都在过原点的一条直线上，或者是构成一个平行四边形格．

54．与问题 14 的论证类似．

55．一个平行六面体格．

56．(i) (2，0，0)，(0，1，0)，(0，0，1)．

(ii) (1，0，0)，(0，3，0)，(0，0，1)．

(iii) (1，0，0)，(0，1，0)，(0，0，5)．

(iv) (2，0，0)，(0，3，0)，(0，0，1)．

(v) 同 (iv)．

(vi) (2，0，0)，(0，3，0)，(0，0，5)．

(vii) 同 (vi)．

57．(i) 2；(ii) 3；(iii) 5；(iv)和 (v) 6；(vi)和 (vii) 30．

58．与问题 57 答案相同．

59．当 $(a,b,c)\in G$ 时，$(x,y,z)\to(x,y,z)+(a,b,c)$是 G 的一个平移．

60．每个点都在这个格的某个平行六面体中，所以可以用格的一个平移将它映射成基本平行六面体中的一点．

61．整个三维空间．若两个像相交，则必重合．

62．$x=0,1$；$y=0,1,2$；$z=0,1,2,3,4$．共30个点．

63．与注记17的论证相似．

64．若两个像相交，则必重合．是的．

65．平移τ将$\Pi\cap\tau^{-1}(V)$映射成$\tau(\Pi)\cap V$．

所有$\tau(\Pi)$的集合填满空间．

所有$\tau^{-1}(V)$的集合填满空间．

66．$<A,B,C>$的陪集个数

= 基本区域中的格点数

= 最小顶点在基本区域中的单位立方体个数

= 这些单位立方体的体积之和

= 平行六面体的体积．

67．三维空间的开域是这样一个区域，它含有它的每个点的一个球邻域．

(iv)，(vi)和(viii)．

68．若三维空间的开域R的体积是V，含有点$(0,0,0)$，并且它在$\mathbf{Z}^3$的平移之下的像都不相交，则当R是在立方体$|x|$，$|y|$，$|z|<r$内时，必有$V\leqslant 1$．

69．(i)球；(ii)半球；(iii)一对半径相等并且相切的球；(iv)一对半径不同但相切的球．

70．设R是空间中的凸区域，关于点O对称，并且与它在把O变为A的平移之下的像相交，那么，将R以点O为中心放大二倍后就包含A．

71．设R是空间中的凸区域，关于点$(0,0,0)$对称，并且体积大于8，那么，R含有$\mathbf{Z}^3$的一个不同于$(0,0,0)$的格点．

74．$15x^2+14y^2-71z^2\equiv 14y^2-71z^2 \pmod 3$，

再若$y\equiv z \pmod 3$，则$14y^2-71z^2\equiv -57z^2\equiv 0 \pmod 3$．

$$15x^2+14y^2-71z^2\equiv 14y^2-71z^2 \pmod 5,$$

再若$z\equiv 2y \pmod 5$，则$14y^2-71z^2\equiv 14y^2-284y^2\equiv -270y^2\equiv 0 \pmod 5$．

体积是 15.

75. $15x^2+14y^2-71z^2\equiv 15x^2-71z^2 \pmod 7$,

再若 $x\equiv z \pmod 7$,则 $15x^2-71z^2\equiv -56z^2\equiv 0 \pmod 7$.

$$15x^2+14y^2-71z^2\equiv 15x^2+14y^2 \pmod{71},$$

再若 $y\equiv 2x \pmod{71}$,则 $15x^2+14y^2\equiv 71x^2\equiv 0 \pmod{71}$.

体积是 497.

76. $y\equiv 0 \pmod 2 \Rightarrow y^2\equiv 0 \pmod 4 \Rightarrow 14y^2\equiv 0 \pmod 8$

$$15x^2-71z^2\equiv 7x^2-7z^2\equiv (x-z)(x+z) \pmod 8.$$

若 $x\equiv z \pmod 4$,则 $x-z$ 有因数 4,从而 x 与 z 同为奇数或偶数.所以 $x+z$ 有因数 2,于是 $(x-z)(x+z)\equiv 0 \pmod 8$.

77. $3\cdot 5\cdot 7\cdot 71\cdot 4\cdot 2=4\cdot 15\cdot 14\cdot 71$.

78. 与问题 44 类似.

80. 若 $|15x_1^2+14y_1^2-71z_1^2|<k$ 且 $15x_1^2+14y_1^2-71z_1^2\equiv 0 \pmod k$,则 $15x_1^2+14y_1^2-71z_1^2=0$.

81. 因为 $\gcd(x,y,z)=1$,所以它们不可能都是偶数.若有两个是偶数,则三个都是偶数,所以至多一个是偶数.若 x,y 是奇数,则 $3x^2$ 与 $5y^2$ 都是奇数,所以 $3x^2+5y^2$ 是偶数,因而 z 必是偶数.三个数不能都是奇数.只有一个是偶数.

82. 若 x 是偶数,则 $5y^2=62z^2-3x^2$ 是偶数,从而 y 是偶数,于是 $3x^2+5y^2$ 有因数 4,所以 z 是偶数,这与 $\gcd(x,y,z)=1$ 矛盾.对于 y 可同样讨论,所以 x,y 都是奇数.若 $x=2n+1$,则 $x^2=4n^2+4n+1=4n(n+1)+1$.但 n 与 $n+1$ 中有一个是偶数,所以 $x^2\equiv 1 \pmod 8$.因此 $3x^2+5y^2\equiv 0 \pmod 8$,从而 $62z^2\equiv 0 \pmod 8$,$31z^2\equiv 0 \pmod 4$.于是,z 是偶数.

对于任何两个奇数 x,y,必有 $x\equiv \pm y \pmod 4$.

83. 与问题 82 类似,可以证明 x 与 y 都是奇数,因此 $x^2\equiv y^2\equiv 1 \pmod 8$.

于是 $2z^2\equiv 3+7 \pmod 8$,所以 $z^2\equiv 1 \pmod 8$,z 是奇数.

与问题 82 类似，得到 $x \equiv \pm y \pmod 4$．

84．(i) 因为 $\gcd(ax_1, by_1, cz_1, 4abc)=1$，所以在 ax_1, by_1 中至多有一个偶数．若 ax_1 是偶数，则 ax_1^2 也是偶数．因此，由 $by_1^2 \equiv -cz_1^2 - ax_1^2 \pmod 8$ 可知 by_1^2 是偶数，所以 by_1 也是偶数．

(ii) 若 ax_1 是奇数，则 x_1 是奇数．因而 $x_1^2 \equiv y_1^2 \equiv 1 \pmod 8$，所以 $ax_1^2 + by_1^2 + cz_1^2 \equiv a + b + cz_1^2 \equiv 0 \pmod 8$．因此，若 z_1 是偶数，则 $a+b \equiv 0 \pmod 8$．

(iii) 若 z_1 是奇数，则 $z_1^2 \equiv 1 \pmod 8$，于是 $a+b+c \equiv 0 \pmod 8$．

若 $x \equiv y \equiv 0 \pmod 4$，则 z 是偶数，并且 ax^2, by^2 以及 cz^2 都同余于 $0 \pmod 8$．

若 $x \equiv y \equiv 2 \pmod 4$ 且 z_1 是偶数，则 $ax^2 + by^2 + cz^2 \equiv 4a + 4b \equiv 0 \pmod 8$．

若 $x \equiv y \equiv 2 \pmod 4$ 且 z_1 是奇数，则 $ax^2 + by^2 + cz^2 \equiv 4a + 4b + 4c \equiv 0 \pmod 8$．

若 $x \equiv y \equiv \pm 1 \pmod 4$ 且 z_1 是偶数，则 $ax^2 + by^2 + cz^2 \equiv a + b \equiv 0 \pmod 8$．

若 $x \equiv y \equiv \pm 1 \pmod 4$ 且 z_1 是奇数，则 $ax^2 + by^2 + cz^2 \equiv a + b + c \equiv 0 \pmod 8$．

85．因为 $p \mid a$，所以 $by_1^2 + cz_1^2 \equiv 0 \pmod p$．如果这两项中有一项有因数 p，那么另一项也有因数 p，但这就与 $\gcd(ax_1, by_1, cz_1, 4abc)=1$ 矛盾．因为 z_1 没有因数 p，所以存在整数 k，使得 $kz_1 \equiv 1 \pmod p$．可取 $l = y_1 k$．

86．对于 $4abc$ 的每个素因数，对应着一个格；这些格的交集，就是所求的格．

对于 a, b 或 c 的每个奇素因数 p，按照注记 85 那样构造一个格 $y = lz \pmod p$，或 $z \equiv lx$，或 $x \equiv lz \pmod p$．因为 ax_1, by_1, cz_1 中恰好有一个偶数，所以 a, b, c 中至多有一个偶数。设 c 是偶数，则问题 84 已指出怎样去构造所需要的指数为 8 的格．若 a, b，

c 都是奇数，则 z_1 是偶数，于是 $a+b\equiv 0 \pmod 4$，那么我们可取由 $x\equiv y \pmod 2$ 和 $z\equiv 0 \pmod 2$ 所确定的指数为4 的格.椭球的体积是 $\frac{4}{3}\pi\cdot 8|abc|>8\cdot 4|abc|$，而根据问题 73，它含有异于原点的格点，这个点满足 $ax^2+by^2+cz^2\equiv 0 \pmod{4abc}$ 以及 $|ax^2+by^2+cz^2|<4|abc|$，所以 $ax^2+by^2+cz^2=0$.

此处所证明的结论不同于最常见的Legendre 定理的形式. Nagell (1964 年)给出了三种形式. L. J. Mordell 在 *Journal of Number Theory* (1969)第一卷中给出了下述命题的一个简单的证明：若 $ax^2+by^2+cz^2=0$ 有解，则它有一个解满足条件 $|x|<\sqrt{|bc|}$，$|y|<\sqrt{|ca|}$，$|z|<\sqrt{|ab|}$.

历史注记

第一次利用格来得到数论结果，是F. M. G. Eisenstein 在1844 年所作出的贡献，他证明了二次互反律(即我们在第四章中所采用的证明). 但是，使几何发展成为今天这样强有力工具的，却是H. Minkowski. 他的定理首次发表于 1891 年，我们讨论了它的最简单的形式.

1785 年，A. M. Legendre 证明，若 a,b,c 两两互素，都不等于零，也都不被平方数整除，那么 $ax^2+by^2+cz^2=0$ 有不全为零的整数解的充要条件，是 $-bc$，$-ac$ 以及 $-ab$ 分别是模 a,b 以及 c 的二次剩余，而且 a,b,c 的正负号不全相同. 数的几何对二次型的应用，是由 Eisenstein 提出，Minkowski 所发展的.

第十章　连 分 数

本章和下一章都要用到袖珍计算器.

无理平方根

1. 设 a 和 b 是正实数且 $\frac{a}{b}=\sqrt{2}$,证明 $\frac{2b-a}{a-b}=\sqrt{2}$ 及 $b>b-a>0$.

用 Fermat 递降法证明 a 和 b 不能都是整数.

2. 设 a 与 b 是正实数且 $\frac{a}{b}=\sqrt{7}$,证明 $\frac{7b-2a}{a-2b}=\sqrt{7}$ 及 $b>a-2b>0$.进而推出 a 和 b 不能都是整数.

3. 仿照问题 1 和问题 2 中的构造方法,证明 $\sqrt{57}$ 不是有理数.

4. 求整数 a,b,c,d,使得 $\frac{2520}{735}=2^a3^b5^c7^d$.

5. 设 $p_1,p_2,p_3,\cdots$ 是由全体不同的素数组成的数列,证明每个非零有理数都可表示成 $\pm p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$,其中 n 是某个自然数,并且整数 $a_1,\cdots,a_n$ 唯一地确定.

6. 设 $r=\pm p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$,那么 r^2 的这种表示式中的指数是怎样的?

7. 2,3,5,6 能是有理数的平方吗?

收 敛 性

连分数的概念起源于寻求无理平方根的有理数逼近的尝试.

8. 证明$\sqrt{2}=1+\dfrac{1}{1+\sqrt{2}}$,并由此推出

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{1+\sqrt{2}}}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\sqrt{2}}}}.$$

9. 通常,数

$$1,\quad 1+\frac{1}{2},\quad 1+\cfrac{1}{2+\cfrac{1}{2}},\quad 1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}},$$

$$1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}}$$

也写成

$$1,\quad 1+\frac{1}{2},\quad 1+\frac{1}{2+}\ \frac{1}{2},\quad 1+\frac{1}{2+}\ \frac{1}{2+}\ \frac{1}{2},$$

$$1+\frac{1}{2+}\ \frac{1}{2+}\ \frac{1}{2+}\ \frac{1}{2}$$

或者

[1],[1,2],[1,2,2],[1,2,2,2],[1,2,2,2,2].

(i) 将这五个数都写成整数的商.

(ii) 设$\dfrac{a}{b}$与$\dfrac{c}{d}$是(i)中相邻的两项,求四种可能出现的

$ad-bc$.

(iii) 用计算器把这五个数表示成十进位小数，观察这个数列是增加的，减少的，还是振荡的，以及它是否好像是在逼近 $\sqrt{2}$？

10. 对于实数 $a_1, a_2, a_3, \cdots, a_n$，用 $[a_1, a_2, \cdots, a_n]$ 表示简单连分数

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{\ddots\ \cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}}}}.$$

通常要求 $a_i \geqslant 1\ (i \geqslant 2)$. 把

$$[1,x],[1,2],\left[1,2+\frac{1}{y}\right],[1,2,y],[1,2,3],\left[1,2,3+\frac{1}{z}\right],$$

$$[1,2,3,z],[1,2,3,4],\left[1,2,3,4+\frac{1}{u}\right],[1,2,3,4,u]$$

写成商的形式.

设 $\frac{a}{b}$ 和 $\frac{c}{d}$ 是数列 $[1],[1,2],[1,2,3],[1,2,3,4],[1,2,3,4,5]$ 中的相邻两项，求四种可能情形中的 $ad-bc$.

11. 设 $[1,2,3,\cdots,9,10]=\frac{p}{q}$ 且 $[1,2,3,\cdots,9,10,11]=\frac{r}{s}$，利用问题 10，试猜测 $[1,2,3,\cdots,9,10,11,x]$ 之值.

12. 记 $p_1=1, p_2=3, p_n=np_{n-1}+p_{n-2}\quad (n\geqslant 3)$,
$q_1=1, q_2=2, q_n=nq_{n-1}+q_{n-2}\quad (n\geqslant 3)$.

验证

$$[1,2,x]=\frac{xp_2+p_1}{xq_2+q_1},\quad [1,2,3,x]=\frac{xp_3+p_2}{xq_3+q_2},$$

并用归纳法证明

$$[1,2,3,\cdots,n-1,x]=\frac{xp_{n-1}+p_{n-2}}{xq_{n-1}+q_{n-2}},$$

13．记 $p_1=a_1, p_2=a_1a_2+1, p_n=a_np_{n-1}+p_{n-2}\quad(n\geqslant 3)$，
$q_1=1, q_2=a_2, q_n=a_nq_{n-1}+q_{n-2}\quad(n\geqslant 3)$，

验证

$$[a_1,a_2,x]=\frac{xp_2+p_1}{xq_2+q_1},\quad [a_1,a_2,a_3,x]=\frac{xp_3+p_2}{xq_3+q_2}.$$

用归纳法证明

$$[a_1,a_2,\cdots,a_{n-1},x]=\frac{xp_{n-1}+p_{n-2}}{xq_{n-1}+q_{n-2}},$$

并推导 $[a_1,a_2,\cdots,a_n]=\dfrac{p_n}{q_n}$.

14．使用上题的记号，若 $a_1,a_2,\cdots,a_n$ 是正整数，$\dfrac{p_n}{q_n}$ 是否必为有理数？

15．使用问题 13 的记号．

(i) 证明 $p_nq_{n-1}-p_{n-1}q_n=-(p_{n-1}q_{n-2}-p_{n-2}q_{n-1})$；

(ii) 求 $p_2q_1-p_1q_2$ 之值；

(iii) 推导 $p_nq_{n-1}-p_{n-1}q_n=(-1)^n$.

16．设 a, m, n, u, v 是正实数且 $\dfrac{m}{n}<\dfrac{u}{v}$，证明

$$\frac{m}{n}<\frac{am+u}{an+v}<\frac{u}{v}$$

与

$$\frac{m}{n}<\frac{m+au}{n+av}<\frac{u}{v}.$$

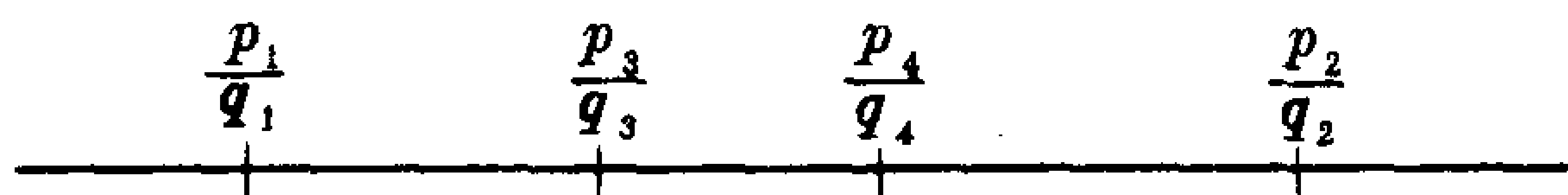
17．使用问题 13 的记号，数列

$$\frac{p_1}{q_1},\ \frac{p_2}{q_2},\ \cdots,\ \frac{p_n}{q_n}$$

的每一项是否介于它前面的两个项之间？利用

$$\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}=\frac{(-1)^n}{q_{n-1}q_n},$$

证明数列的每个偶数项（即项 $\frac{p_{2l}}{q_{2l}}$）都大于它前面的一项，而每个奇数项（即项 $\frac{p_{2l+1}}{q_{2l+1}}$）则小于它前面的一项．



每个奇数项是否都小于每个偶数项？

18．从有理数 $\frac{61}{48}$ 出发，利用计算器验证

$$\frac{61}{48}=[1,3,1,2,4].$$

数 [1]，[1，3]，[1，3，1]，[1，3，1，2]，[1，3，1，2，4] 都称为 $\frac{61}{48}$ 的渐近分数．

把每个渐进分数写成整数之商的形式，并利用倒数第二个渐近分数求整数 x,y，使得 $61x-48y=-1$．

证明 $[1,3,1,2,4]=[1,3,1,2,3,1]$．

计算 $[1,3,1,2,3]$，并求整数 x,y，使得 $61x-48y=1$．

你所求得的 x 是小于 48 的正整数，y 是小于 61 的正整数，证

明它们是满足方程的最小正整数.

19. 利用等式

$$168=2\cdot 73+22,$$
$$73=3\cdot 22+7,$$
$$22=3\cdot 7+1,$$
$$7=7\cdot 1,$$

求整数 a_1,a_2,a_3,a_4 使得

$$\frac{168}{73}=[a_1,a_2,a_3,a_4].$$

计算 $[a_1,a_2,a_3]$ 并求 $168x-73y=1$ 的一组整数解.

b 取何值时, $\frac{168}{73}=[a_1,a_2,a_3,b,1]$?

计算 $[a_1,a_2,a_3,b]$, 并求 $168x-73y=-1$的一组整数解.

20. 求正整数 $b_1,b_2,b_3,b_4,r_1,r_2,r_3$,使得$25>r_1>r_2>r_3$,而且

$$217=2\cdot 96+25,$$
$$96=b_1\cdot 25+r_1,$$
$$25=b_2\cdot r_1+r_2,$$
$$r_1=b_3\cdot r_2+r_3,$$
$$r_2=b_4\cdot r_3,$$

利用这些数值,求整数 a_1,a_2,a_3,a_4,a_5,使得 $\frac{217}{96}=[a_1,a_2,a_3,a_4,a_5]$.

21. 设 a,b 是互素的正整数,对于某个正整数 n,是否一定存在 $a_1,a_2,\cdots,a_n$,使得

$$\frac{a}{b}=[a_1,a_2,\cdots,a_n]$$

(其中只有 a_1 可能为零)? 给定 a 和 b,如何求 a_i?

22. 设 $[a_1,a_2,\cdots,a_n]=[b_1,b_2,\cdots,b_m]$,其中的项除 a_1,b_1 外都是正整数,a_1 与 b_1 可以是任意整数. 证明:若 $m,n\geqslant 2$,则

$[a_2,\cdots,a_n]$ 与 $[b_2,\cdots,b_m]$ 都大于 1，因而

$$\frac{1}{[a_2,\cdots,a_n]} \text{ 与 } \frac{1}{[b_2,\cdots,b_m]}$$

都小于 1.

证明 a_1 和 b_1 分别是开头的等式两边的数的整数部分，因此 $a_1=b_1$ 且 $[a_2,\cdots,a_n]=[b_2,\cdots,b_m]$. 若 $n\leqslant m$，将此论证重复 n 次，则可推出 $a_i=b_i\ (i<n)$ 及 $[a_n]=[b_n,\cdots,b_m]$. 这是一个关于整数的等式，所以 $n=m$，$a_n=b_n$，或者是 $n+1=m$，$a_n=b_n+1$，$b_m=b_{n+1}=1$.

23. 令 $a_1=[\sqrt{3}]$（见问题4.44），再用 $\sqrt{3}=[a_1,x_2]$ 定义 x_2.

令 $a_2=[x_2]$（见问题4.44），再用 $\sqrt{3}=[a_1,a_2,x_3]$ 定义 x_3.

令 $a_3=[x_3]$（见问题4.44），再用 $\sqrt{3}=[a_1,a_2,a_3,x_4]$ 定义 x_4.

一般地，令 $a_{n-1}=[x_{n-1}]$，并且 $\sqrt{3}=[a_1,a_2,\cdots,a_{n-1},x_n]$ 定义 x_n.

利用 $\sqrt{3}=1+\cfrac{1}{1+\cfrac{1}{1+\sqrt{3}}}$，

求 $a_1,a_2,a_3,a_4,a_5,a_6,a_7$. 有理数 $[a_1]$，$[a_1,a_2]$，$\cdots$，$[a_1,a_2,a_3,\cdots,a_n]$ 称为 $\sqrt{3}$ 的前 n 个渐近分数.

求 $\sqrt{3}$ 的前五个渐近分数并将它们依次标在数轴上.

$\sqrt{3}$ 是否必有无限多个渐近分数？

24. 对任一无理数 x，令 $a_1=[x]$（见问题4.44），并用 $x=[a_1,x_2]$ 定义 x_2；令 $a_2=[x_2]$（见问题4.44）. 并用 $x=[a_1,a_2,x_3]$ 定义 x_3.

依次逆推，令 $a_{n-1}=[x_{n-1}]$，并用 $x=[a_1,a_2,\cdots,a_{n-1},x_n]$ 定义 x_n.

将 $[a_1]$，$[a_1,a_2]$，$\cdots$，$[a_1,a_2,\cdots,a_n]$ $\cdots$ 称为 x 的渐近分数.

说明
$$0<\frac{1}{x_2}<1\quad,\ x_2>1\ ,$$
$$0<\frac{1}{x_3}<1\quad,\ x_3>1$$
的理由，并证明 $a_2, a_3, \cdots$ 都是正整数．

记 $c_n=[a_1, a_2, \cdots, a_n]$，利用问题 17 推出
$$c_1<c_3<c_5<c_6<c_4<c_2\ .$$
使用问题 13 的记号，证明
$$x=\frac{x_n p_{n-1}+p_{n-2}}{x_n q_{n-1}+q_{n-2}}\quad,$$
而且 x 落在任何两个相邻渐近分数之间：
$$c_1<c_3<c_5<x<c_6<c_4<c_2\ .$$
利用问题 17，证明
$$\left|x-\frac{p_n}{q_n}\right|<\frac{1}{q_n q_{n+1}}\ .$$
因为$\{q_n\}$是递增的无界正整数列，所以这就证明了 $\frac{p_n}{q_n}\to x$ $(n\to\infty)$．

25．从任何一个无限连分数$[a_1, a_2, \cdots, a_n, \cdots]$出发，其中 a_1 是整数，$a_i\ (i>1)$是正整数，可以构造一个渐近分数列

$c_1=[a_1]=a_1$，

$c_2=[a_1, a_2]$，

$c_3=[a_1, a_2, a_3]$，

⋮

$c_n=[a_1, a_2, \cdots, a_n]$，

⋮

利用问题 17 证明：由奇数项渐近分数构成的子序列 (c_{2n+1})

单调增加且有上界，由偶数项渐近分数构成的子序列 (c_{2n}) 单调减小且有下界，因而它们都有极限．利用问题 17 证明这两个极限必相等，设 $(c_n)\to\alpha\ (n\to\infty)$，利用所有的 c_n 的整数部分都是 a_1 这个事实，证明 $[\alpha]=a_1$．利用同样的论证，证明 $[a_1, a_2, \cdots, a_n, \cdots]$ 就是问题 24 中所定义的 α 的连分数．

纯循环连分数

我们知道，每个简单连分数收敛于唯一的实数．现在，我们来研究那些 $a_1, a_2, \cdots, a_n, \cdots$ 是纯循环数列的连分数，看看它们的极限是什么样的实数．

26．设 $\alpha=[1, 1, 1, \cdots]$，利用 $\alpha=[1, \alpha]$，证明 $\alpha^2-\alpha-1=0$，并由此求 α 值．

27．设 $\alpha=[2, 2, 2, \cdots]$，利用 $\alpha=[2, \alpha]$，证明 $\alpha^2-2\alpha-1=0$.

28．设 $\alpha=[a, a, a, \cdots]$，此处 a 是正整数，利用 $\alpha=[a, \alpha]$，找一个 α 所满足的二次方程以及求 α 的公式．

29．设 $\alpha=[1, 2, 1, 2, 1, \cdots]$，利用 $\alpha=[1, 2, \alpha]$ 证明 $2\alpha^2-2\alpha-1=0$ 并由此求 α 值．

30．设 $\beta=[2, 1, 2, 1, 2, \cdots]$，简记为 $\beta=[\dot{2}, \dot{1}]$，利用 $\beta=[2, 1, \beta]$ 证明 $\beta^2-2\beta-2=0$，并由此求 β 值．证明 $2x^2-2x-1=0$ 的根是 $[\dot{1}, \dot{2}]$ 与 $-\dfrac{1}{[\dot{2}, \dot{1}]}$．

31．设 $\alpha=[a, b, a, b, \cdots]$，简记为 $\alpha=[\dot{a}, \dot{b}]$，其中 a, b 是正整数，找一个 α 所满足的二次方程．证明这个二次方程有一个正根和一个负根．找一个被 $[b, a, b, a, \cdots]=[\dot{b}, \dot{a}]$ 所满足的二次方程，并证明 $[\dot{a}, \dot{b}]$ 与 $-\dfrac{1}{[\dot{b}, \dot{a}]}$ 满足同一个整系数二次方程．

32．设 $\alpha=[a, b, c, a, b, c, \cdots]$，简记为 $\alpha=[\dot{a}, \dot{b}, \dot{c}]$，其中 a，b，c 都是正整数，找一个 α 所满足的整系数二次方程．写出 $[c, b,$

$a, c, b, a, \cdots]$ 所满足的一个二次方程，并证明 $[\dot{a}, b, \dot{c}]$ 与 $-1/[\dot{c}, b, \dot{a}]$ 是同一个整系数二次方程的根.

33. 设 $\alpha=[a_1, a_2, \cdots, a_n, \alpha]$，其中 $a_1, a_2, \cdots, a_n$ 是正整数，再设 $[a_1, a_2, \cdots, a_{n-1}]=\dfrac{p_{n-1}}{q_{n-1}}$ 且 $[a_1, a_2, \cdots, a_n]=\dfrac{p_n}{q_n}$，利用问题 13 证明 α 满足一个整系数二次方程.

证明：任何一个纯循环连分数（例如 $[\dot{a}_1, a_2, \cdots, \dot{a}_n]$，其中 $a_1, a_2, \cdots, a_n$ 都是正整数）满足一个整系数二次方程.

34. 使用问题 13 的记号，证明

$$p_2/p_1=[a_2, a_1], \quad p_3/p_2=[a_3, a_2, a_1].$$

利用等式 $p_n=a_np_{n-1}+p_{n-2}$ $(n\geqslant 3)$ 及归纳法，证明当 $n\geqslant 2$ 时，

$$p_n/p_{n-1}=[a_n, a_{n-1}, \cdots, a_1].$$

35. 使用问题 13 的记号，证明

$$q_2/q_1=a_2, \quad q_3/q_2=[a_3, a_2].$$

利用等式 $q_n=a_nq_{n-1}+q_{n-2}$ $(n\geqslant 3)$ 及归纳法，证明，当 $n\geqslant 2$ 时，

$$q_n/q_{n-1}=[a_n, a_{n-1}, \cdots, a_2].$$

36. 设 $\alpha=[\dot{a}_1, a_2, \cdots, \dot{a}_n]$，$\beta=[\dot{a}_n, a_{n-1}, \cdots, \dot{a}_1]$，其中 a_i 都是正整数，再设

$$p_i/q_i=[a_1, a_2, \cdots, a_i] \quad (i\leqslant n),$$

证明

$$\alpha=\frac{\alpha p_n+p_{n-1}}{\alpha q_n+q_{n-1}}, \quad \beta=\frac{\beta p_n+q_n}{\beta p_{n-1}+q_{n-1}}.$$

求出 α 与 β 所满足的整系数二次方程.

37. 设 $\alpha=[\dot{a}_1, a_2, \cdots, \dot{a}_n]$，利用问题 36 推导：由 $\alpha=[a_1, a_2, \cdots, a_n, \alpha]$ 所得到的二次方程的根是 α 和 $-\dfrac{1}{\beta}$. 利用诸 a_i 都是正整数，证明这两个根中一个大于 1，另一个在 -1 与 0 之间.

38. 求一个以 $1+\sqrt{2}$ 为根的整系数二次方程. 它的另一个

根是什么？还有没有别的这样的方程？若有，那么这个方程的另一个根是什么？

39. 用 $\mathbf{Q}(\sqrt{2})$ 表示所有形如 $a+b\sqrt{2}$ 的数所成的集合，其中 a,b 是有理数. 若 $b\neq 0$，这种数是否都是某个整系数二次方程的根？

40. 设 a,b 是有理数，$a+b\sqrt{2}=0$，证明 a 和 b 都等于 0.

设 a,b,c,d 是有理数，$a+b\sqrt{2}=c+d\sqrt{2}$，证明 $a=c$，$b=d$.

41. $\mathbf{Q}(\sqrt{2})$ 中两数的和、差、积、商是否都仍在此集合内（当然不包括除数为零的情形）？

42. 设 a,b 是有理数，$a+b\sqrt{2}$ 是方程 $px^2+qx+r=0$ 的根，其中 p,q,r 都是整数，那么 $a-b\sqrt{2}$ 是否也是这个方程的根？

43. 设 a,b 是有理数，$\alpha=a+b\sqrt{2}$，我们用 $\overline{\alpha}$ 表示 α 的**共轭数** $a-b\sqrt{2}$.

对于一切 $\alpha,\beta\in\mathbf{Q}(\sqrt{2})$，是否有

$\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$？

$\overline{\alpha\beta}=\overline{\alpha}\ \overline{\beta}$？

$\overline{\left(\frac{1}{\alpha}\right)}=\frac{1}{\overline{\alpha}}\quad(\alpha\neq 0)$？

44. 若将 $\sqrt{2}$ 换成 $\sqrt{d}$，此处 d 是任一非平方正整数，那么在问题 39—43 中所得到的结果是否仍成立？

45. 设 $1+\sqrt{2}=\alpha$，求 α_2 使得 $\alpha=[\alpha]+\frac{1}{\alpha_2}$.

验证 α 与 α_2 是否都大于 1，以及它们的共轭数是否都在 -1 与 0 之间.

46. 设 $2+\sqrt{7}=\beta$，求 β_2 使得 $\beta=[\beta]+\frac{1}{\beta_2}$.

验证 β 与 β_2 是否都大于 1，以及它们的共轭数是否都在 -1 与 0 之间.

分别求 β 与 β_2 所满足的整系数二次方程．

比较这两个方程的判别式．

47．设 α 是 $\mathbf{Q}(\sqrt{d})$ 中的无理数，$\alpha=[\alpha]+\dfrac{1}{\alpha_2}$，证明 α_2 也是 $\mathbf{Q}(\sqrt{d})$ 中的无理数．此外，若 $\alpha>1$ 且 $-1<\overline{\alpha}<0$，证明 $\alpha_2>1$ 且 $-1<\overline{\alpha_2}<0$．

48．推广问题 38 的论证可以证明：$\mathbf{Q}(\sqrt{d})$ 中的每个无理数都是一个整系数二次方程的根，除相差一个整数倍数外，这个方程是唯一的．设 $\alpha=n+\dfrac{1}{\alpha_2}$，此处 α 是 $\mathbf{Q}(\sqrt{d})$ 中的无理数，n 是整数，再设 $a\alpha^2+b\alpha+c=0$ 且 $a'\alpha_2^2+b'\alpha_2+c'=0$，其中 a,b,c 是互素的整数，a',b',c' 也是互素的整数，证明

$$b^2-4ac=b'^2-4a'c'.$$

49．设 $\alpha=(p+\sqrt{2})/q$，那么整数 p 与 q 取何值时，一定有 $\alpha>1$ 且 $-1<\overline{\alpha}<0$？

50．设 $\alpha=(p+\sqrt{11})/q$，那么整数 p 与 q 取何值时，一定有 $\alpha>1$ 且 $-1<\overline{\alpha}<0$？

51．设 $\alpha=(p+\sqrt{d})/q$，其中 p,q 是整数，且 $\alpha>1$，$0>\overline{\alpha}>-1$，证明 $\sqrt{d}>p>0$ 及 $2\sqrt{d}>q>0$，因此，所给的条件使得 p 与 q 只能取有限多个整数值．

52．所谓二次无理数是指这样的实数，它是整系数二次方程的解，但不是有理数．

在问题 37 中已经证明，每个纯循环连分数收敛于一个二次无理数 α．满足 $\alpha>1$，$0>\overline{\alpha}>-1$，下面将证明其逆命题．

设 α 是一个二次无理数，满足 $\alpha>1$，$0>\overline{\alpha}>-1$，证明存在正整数 p,q,d，其中 d 是非平方数，使得 $\alpha=(p+\sqrt{d})/q$．

53．设 d 是非平方正整数，p 和 q 是整数，$\alpha=(p+\sqrt{d})/q$，$\alpha>1$，$0>\overline{\alpha}>-1$，证明

(i) 若 $\alpha=[a_1,\alpha_2]$，其中 $a_1=[\alpha]$，则 $\alpha_2=(p_1+\sqrt{d})/q_1$，其

中 p_1 和 q_1 是整数 (利用问题 48)；

(ii) 若 $\alpha=[a_1, a_2, \alpha_3]$，其中 $a_2=[\alpha_2]$，则 $\alpha_3=(p_2+\sqrt{d})/q_2$，其中 p_2 和 q_2 是整数；

(iii) 若 $\alpha=[a_1, a_2, \cdots, a_{n-1}, \alpha_n]$，其中 $a_{n-1}=[\alpha_{n-1}]$，则 $\alpha_n=(p_{n-1}+\sqrt{d})/q_{n-1}$，其中 p_{n-1} 与 q_{n-1} 是整数；

(iv) 每个 $\alpha_i>1$ 且 $0>\overline{\alpha_i}>-1$ (利用问题 47)；

(v) 只有有限多个不同的 α_i (利用问题 51)；

(vi) 若 $\alpha_n=\alpha_m$ $(1\leqslant n\leqslant m)$是第一次重复出现的两个数，则 $\alpha_{n+1}=\alpha_{m+1}$，进而利用归纳法得到 $\alpha_{n+i}=\alpha_{m+i}$ 对一切正整数 i 成立；

(vii) 若 $\beta_n=-1/\overline{\alpha}_n$，则对一切 n 有 $\beta_n>1$；

(viii) 若 $n>1$，则 $\beta_n=a_{n-1}+1/\beta_{n-1}$，所以 $a_{n-1}=[\beta_n]$；

(ix) 因为 $\beta_n=\beta_m$，所以 $[\beta_n]=[\beta_m]$，且 $\beta_{n-1}=\beta_{m-1}$，于是 $\alpha_{n-1}=\alpha_{m-1}$，因此 $n=1$。

Pell 方程

对于纯循环连分数与二次无理数的关系，我们已经有了确切的了解。现在，我们能利用它确定哪些二次无理数是这样的连分数的极限：它们是从第二项开始是循环的。首先，我们来确定正整数的平方根的连分数，并利用所得到的结果去解 Pell方程 $x^2-dy^2=1$。

54. 整数 n 取何值时，$n+\sqrt{2}>1$ 且 $0>n-\sqrt{2}>-1$？对于这个 n 值，写出 $n+\sqrt{2}$ 的循环连分数，进而导出 $\sqrt{2}$ 的连分数。

55. 重复问题 54 的方法，求 $\sqrt{3}$，$\sqrt{5}$，$\sqrt{6}$ 和 $\sqrt{7}$ 的连分数。

56. 设 d 是非平方正整数，$[\sqrt{d}]+\sqrt{d}$ 是否必有一个纯循环连分数的展开式？

57. 利用上题说明：若 d 是非平方正整数，则 $\sqrt{d}$ 的连分数

从第二项开始是循环的.

58. 为什么 $5+\sqrt{33}$ 一定给出一个纯循环连分数?

设 $5+\sqrt{33}=[\dot{a}_1,\dot{a}_2,\cdots,\dot{a}_n]$,其中 a_i 是正整数,那么 a_1 等于多少?

证明 $\sqrt{33}=[5,\dot{a}_2,\dot{a}_3,\cdots,\dot{a}_n,1\dot{0}]$,

因而

$$\sqrt{33}-5=[0,\dot{a}_2,\dot{a}_3,\cdots,\dot{a}_n,1\dot{0}],$$

$$\frac{1}{\sqrt{33}-5}=[\dot{a}_2,\dot{a}_3,\cdots,\dot{a}_n,1\dot{0}].$$

利用问题 37 及问题 42 的推广,证明

$$\frac{1}{\sqrt{33}-5}=[\dot{a}_n,\dot{a}_{n-1},\cdots,\dot{a}_2,\dot{a}_1],$$

因此 $a_2=a_n,a_3=a_{n-1}$,等等.

59. 设 d 是非平方正整数,$\sqrt{d}=[a_1,\dot{a}_2,\dot{a}_3,\cdots,\dot{a}_n]$,试确定 a_1 与 a_n 的关系,以及这一周期中相等的数对.

60. 已知 $\sqrt{14}=[3,\dot{1},\dot{2},\dot{1},\dot{6}]$,证明 $\sqrt{14}=[3,1,2,1,\sqrt{14}+3]$.

进而利用 $[3,1,2]=\frac{11}{3}$ 与 $[3,1,2,1]=\frac{15}{4}$ 推出

$$\sqrt{14}=\frac{(\sqrt{14}+3)15+11}{(\sqrt{14}+3)4+3}.$$

简化并验证这个等式.

61. 设 d 是非平方正整数,$\sqrt{d}=[a_1,\dot{a}_2,\dot{a}_3,\cdots,\dot{a}_n,2\dot{a}_1]$,其中 a_i 是正整数,证明

$$\sqrt{d}=[a_1,a_2,a_3,\cdots,a_n,a_1+\sqrt{d}].$$

设 $[a_1,a_2,\cdots,a_{n-1}]=p_{n-1}/q_{n-1}$ 及 $[a_1,a_2,\cdots,a_n]=p_n/q_n$(见问题 13),证明

$$\sqrt{d} = \frac{(a_1+\sqrt{d})p_n+p_{n-1}}{(a_1+\sqrt{d})q_n+q_{n-1}}.$$

利用问题40的一般形式，证明

$$dq_n = a_1p_n+p_{n-1}, a_1q_n+q_{n-1}=p_n.$$

利用问题15，证明$p_n^2-dq_n^2=(-1)^n$.

62．利用问题60和问题61，求x，y，使得$x^2-14y^2=1$.

63．已知$\sqrt{13}=[3,\dot{1},1,1,\dot{1},\dot{6}]$，利用问题61，求整数$x$，$y$，使得$x^2-13y^2=-1$.

通过计算$\sqrt{13}$在第二个周期中的渐近分数，求整数x，y，使得$x^2-13y^2=1$.

64．对模3考察方程$x^2-3y^2=-1$.证明它没有整数解x，y.

对模6考察方程$x^2-6y^2=-1$，证明它没有整数解x，y.

65．对于哪些非平方整数d，必有非零的整数x，y，使得$x^2-dy^2=1$？（Pell方程）

66．
$$\begin{aligned}3^2-2\cdot 2^2=1 &\Rightarrow (3+2\sqrt{2})(3-2\sqrt{2})=1\\ &\Rightarrow (3+2\sqrt{2})^2(3-2\sqrt{2})^2=1\\ &\Rightarrow (17+12\sqrt{2})(17-12\sqrt{2})=1\\ &\Rightarrow 17^2-2\cdot 12^2=1.\end{aligned}$$

若已知$a^2-2b^2=1$，能否推广这个方法，以得到$x^2-2y^2=1$的另外的整数解？

是否存在无限多对整数x，y，使得$x^2-2y^2=1$？

67．设$a+b\sqrt{2}$是$x^2-2y^2=1$的最小整数解（即，若a，b，x，y是正整数且$a^2-2b^2=x^2-2y^2=1$，则$1<a+b\sqrt{2}\leqslant x+y\sqrt{2}$）.因为$1<a+b\sqrt{2}$，所以$x+y\sqrt{2}$必在$a+b\sqrt{2}$的两个幂之间，假定是$(a+b\sqrt{2})^n\leqslant x+y\sqrt{2}<(a+b\sqrt{2})^{n+1}$，用$(a-b\sqrt{2})^n$乘此不等式两边，证明$x+y\sqrt{2}=(a+b\sqrt{2})^n$.

68．设d是非平方正整数，那么$x^2-dy^2=1$.是否必有无穷多组整数解？所有的解是否一定都可以由最小整数解得到？

69. 设 d 是非平方正整数，a，b 是使 $a^2-db^2=1$ 的最小正整数，证明

$$x=\frac{1}{2}[(a+b\sqrt{d})^n+(a-b\sqrt{d})^n]$$

与
$$y=\frac{1}{2\sqrt{d}}[(a+b\sqrt{d})^n-(a-b\sqrt{d})^n]$$

都是整数，而且 $x^2-dy^2=1$ 的解都是这种形式.

70. 给出 $x^2-2y^2=1$ 的所有整数解的通式，并推出

$$x^2+8xy+14y^2+6x+24y+8=0$$

的所有整数解的公式.

71. 利用问题 55 的答案，求满足 $x^2-5y^2=1$ 的正整数 x，y. 求 $x^2-5y^2=4$ 的两组解，使得一组 x，y 都是正偶数，另一组都是奇数.

设 $a^2-5b^2=4$ 且 $c^2-5d^2=4$，证明 $(ac+5bd)^2-5(ad+bc)^2=16$. 证明：若

$$p+q\sqrt{5}=2\left(\frac{a+b\sqrt{5}}{2}\right)\left(\frac{c+d\sqrt{5}}{2}\right),$$

则 $p^2-5q^2=4$. 设 a，b，c，d 是正整数，证明 p，q 是整数.

利用这种构造解的方法，对方程 $x^2-5y^2=4$，从你已找到的 x，y 都是奇数的解，求出你在前面找到的 x，y 都是偶数的解.

关于二次无理数的 Lagrange 定理

现在我们研究与混循环连分数所对应的无理数. Lagrange 证明，这些数就是全体二次无理数.

72. 设 $\alpha=[1,\dot{2},\dot{3}]$，参照问题 37，求整数 n，使得 $n+\alpha>1$，$0>n+\overline{\alpha}>-1$.

73. 利用问题 53，判断能否找到整数 n，使得 $n+\alpha>1$ 且 $0>$

$n+\overline{\alpha}>-1$,其中 $\alpha=[1,2,\dot{3},\dot{4}]$.

74. 数 $\frac{1}{2}(3+\sqrt{12})$, $3+\sqrt{5}$, $3-\sqrt{5}$, $1+\frac{1}{4}\sqrt{3}$ 的连分数展开式是不是

(i) 纯循环的,

(ii) 从第二项起是循环的,

(iii) 不是前两种情况.

75. 利用问题 37,说明 $\frac{1}{4}\sqrt{3}$ 的连分数

(i) 不是纯循环的,

(ii) 也不是从第二项开始是循环的.

设 $\frac{1}{4}\sqrt{3}=[0,2,\alpha_3]$,证明 $\alpha_3>1$ 且 $0>\overline{\alpha_3}>-1$.进而推出 $\frac{1}{4}\sqrt{3}$ 的连分数从第三项开始是循环的.

76. 设 α 是二次无理数且

$$\alpha=[a_1,a_2,\cdots,a_{n-1},\alpha_n],$$

其中 a_i 是正整数,α_n 是二次无理数,利用问题 13 的记号,这时有

$$\alpha=\frac{\alpha_n p_{n-1}+p_{n-2}}{\alpha_n q_{n-1}+q_{n-2}}.$$

证明

$$\overline{\alpha_n}=-\frac{q_{n-2}(p_{n-2}/q_{n-2}-\overline{\alpha})}{q_{n-1}(p_{n-1}/q_{n-1}-\overline{\alpha})},$$

并利用问题 24,证明当 n 充分大时,$\overline{\alpha_n}$ 近似地等于 $-q_{n-2}/q_{n-1}$.

证明对于充分大的 n,α_n 是循环连分数,因而 α 是混循环连分数.(Lagrange 定理).

77. 在上题中证明了,二次无理数的连分数是混循环的.利用问题 33 及问题 13 证明它的逆命题.

不定型 ax^2-by^2 的自守变换

作为本章结尾，我们用连分数来研究不定二次型 ax^2-by^2，并确定它的自守变换群.

78. $\sqrt{\frac{5}{3}}=[1,\dot{3},\dot{2}]=\frac{1}{3}\sqrt{15}$. 求 $\frac{1}{3}\sqrt{15}$ 的前四个渐近分数 $p_1/q_1, p_2/q_2, p_3/q_3, p_4/q_4$. 令 $\alpha=\frac{1}{3}\sqrt{15}=[1,\alpha_2]=[1,3,\alpha_3]=[1,3,2,\alpha_4]$，求整数 $A_1,B_1,A_2,B_2,A_3,B_3,A_4,B_4$，使得

$$\alpha=\frac{A_1+\sqrt{15}}{B_1}, \qquad \alpha_2=\frac{A_2+\sqrt{15}}{B_2},$$

$$\alpha_3=\frac{A_3+\sqrt{15}}{B_3}, \qquad \alpha_4=\frac{A_4+\sqrt{15}}{B_4}.$$

填出下表：

n	1	2	3	4
$3p_n^2-5q_n^2$				
B_n				

79. $\mathbf{Q}(\sqrt{15})$ 中的元素是否都可表示成 $(A+\sqrt{N})/B$，其中 A,B,N 是适当选取的整数？为什么还可以要求 $B\mid N-A^2$？当 $B\mid N-A^2$ 时，称二次无理数 $(A+\sqrt{N})/B$ 是具有标准形.

设 $\alpha=(A+\sqrt{N})/B$ 是标准形，且 $\alpha=n+\frac{1}{\beta}$，其中 n 是整数，证明存在整数 C 和 D，使得 $\beta=(C+\sqrt{N})/D$ 是标准形. 如果推广问题 78 中 $\alpha_2,\alpha_3,\alpha_4$ 的定义，得到 $\alpha_n=(A_n+\sqrt{15})/B_n$，

那么它是标准形.

将这个标准形代入等式

$$\alpha=\frac{\alpha_n p_{n-1}+p_{n-2}}{\alpha_n q_{n-1}+q_{n-2}}.$$

利用问题 40 的一般形式及问题 15，证明

$$3p_{n-1}^2-5q_{n-1}^2=(-1)^{n+1}B_n.$$

80. 画出 $3x^2-5y^2=3$ 当 $|x|<5$ 时的草图，标出坐标为整数的那些点.

设 $p^2-15k^2=1$，用代数方法证明 (a,b) 在这条曲线上的充要条件是 $(pa+5kb,3ka+pb)$ 在这曲线上.

若 p 与 k 是整数，那么

$$(x,y)\to(x,y)\begin{pmatrix}p & 3k\\ 5k & p\end{pmatrix}$$

是幺模变换吗?

计算矩阵之积

$$\begin{pmatrix}p & 3k\\ 5k & p\end{pmatrix}\begin{pmatrix}3 & 0\\ 0 & -5\end{pmatrix}\begin{pmatrix}p & 5k\\ 3k & p\end{pmatrix},$$

并描述对二次型 $3x^2-5y^2$ 施行所给变换后的结果.

考虑一一对应

$$\begin{pmatrix}p & 3k\\ 5k & p\end{pmatrix}\to p+k\sqrt{15}$$

并利用问题 67 的推理，证明形如

$$(x,y)\to(x,y)\begin{pmatrix}p & 3k\\ 5k & p\end{pmatrix}$$

的幺模变换构成一个无限循环群，即二次型 $3x^2-5y^2$ 的自守变换群,

81．设 a,b 是正整数，$\gcd(a,b)=1$，证明二次型 ax^2-by^2 有无限多个自守变换．

82．设幺模变换

$$(x,y)\to(x,y)\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

是二次型 $3x^2-5y^2$ 的一个自守变换，证明

(i) $ps-qr=\pm 1$，

(ii) $3p^2-5q^2=3$，

(iii) $3r^2-5s^2=-5$，

(iv) $3pr=5qs$．

利用 (i)和 (iv)证明 $(3p^2-5q^2)s=\pm 3p$，以及 $p^2=s^2$．

利用 (ii)和 (iii)证明 $9r^2=25q^2$．

证明$3x^2-5y^2$ 的自守变换的矩阵具有 $\begin{pmatrix} p & 3k \\ 5k & p \end{pmatrix}$ 或 $\begin{pmatrix} p & 3k \\ -5k & -p \end{pmatrix}$ 的形式，其中$p^2-15k^2=1$．

注记与答案

参考书见书目:Olds (1963)，Stark (1978)，Chrystal (1964)．

1．$$\frac{2b-a}{a-b}=\frac{2-\dfrac{a}{b}}{\dfrac{a}{b}-1}=\frac{2-\sqrt{2}}{\sqrt{2}-1}=\sqrt{2}\ .$$

因为 $4>2>1$，$2>\sqrt{2}>1$，所以 $a>b$，$a-b>0$．又因 $2b>\sqrt{2}b=a$，所以 $b>a-b$．

这就证明了，若 $\sqrt{2}$ 可以表示成两个正整数之商，那么还可以表示成另两个正整数之商，并且分母比原先的小．这样，最终我们得到一个分母为 1 的商，$\sqrt{2}$ 就成了整数．

2. $\dfrac{7b-2a}{a-2b}=\dfrac{7-2\dfrac{a}{b}}{\dfrac{a}{b}-2}=\dfrac{7-2\sqrt{7}}{\sqrt{7}-2}=\sqrt{7}$.

因为$9>7>4$,所以$3>\sqrt{7}>2$.于是$\dfrac{a}{b}>2$,$a-2b>0$.由$3>\dfrac{a}{b}$得到$b>a-2b$.

3. 令$\dfrac{a}{b}=\sqrt{57}$.因为$64>57>49$,所以$8>\sqrt{57}>7$,$b>a-7b>0$.现在,$(57b-7a)/(a-7b)=\sqrt{57}$,这就可以用前面的方法了.

4. $a=3$,$b=1$,$c=0$,$d=-1$.

5. 若h和k是非零整数,它们唯一的素因数分解式为$h=\pm p_1^{b_1}p_2^{b_2}\cdots p_m^{b_m}$, $k=\pm p_l^{c_1}p_2^{c_2}\cdots p_l^{c_l}$.则有理数$\dfrac{h}{k}=\pm p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$;其中$n=\max\{m,l\}$,$a_i=b_i-c_i$.若$b_i$与$c_i$中只有一个存在,则$a_i=b_i$或$a_i=-c_i$.

6. 都是偶数.

7. 不能,因为素因数分解式中有奇指数.

9. (i) $\dfrac{1}{1},\dfrac{3}{2},\dfrac{7}{5},\dfrac{17}{12},\dfrac{41}{29}$.

(ii) $ab-bc=-1,1,-1,1$.

(iii) 振荡地逼近$\sqrt{2}$.

"简单连分数"中的"简单"一词,是指重复出现的分子1.

10. $\dfrac{x+1}{x},\dfrac{3}{2},\dfrac{3y+1}{2y+1},\dfrac{3y+1}{2y+1},\dfrac{10}{7},\dfrac{10z+3}{7z+2}$,

$\dfrac{10z+3}{7z+2},\dfrac{43}{30},\dfrac{43u+10}{30u+7},\dfrac{43u+10}{30u+7}$.

$ad-bc=-1,1,-1,1$.

11. $\dfrac{rx+p}{sx+q}$.

12. 设 $[1,2,3,\cdots,n-1,x]=\dfrac{xp_{n-1}+p_{n-2}}{xq_{n-1}+q_{n-2}}$.

令 $x=n+\dfrac{1}{y}$，则

$$[1,2,3,\cdots,n-1,n,y]=\frac{(n+\frac{1}{y})p_{n-1}+p_{n-2}}{(n+\frac{1}{y})q_{n-1}+q_{n-2}}$$

$$=\frac{y(np_{n-1}+p_{n-2})+p_{n-1}}{y(nq_{n-1}+q_{n-2})+q_{n-1}}=\frac{yp_n+p_{n-1}}{yq_n+q_{n-1}}.$$

这说明，由归纳法可证明结论.

13. 证明与问题12类似.无论对连分数的应用研究还是理论研究，这个结论都是一个主要工具，它使我们在研究中可以略去连分数前面的一些项.

14. p_n 与 q_n 的定义保证了它们都是正整数，从而 p_n/q_n 是有理数.

15. (i) $p_nq_{n-1}-p_{n-1}q_n=(np_{n-1}+p_{n-2})q_{n-1}-p_{n-1}(nq_{n-1}+q_{n-2})$.

(ii) 1.

(iii) (i)的结果表明，对于 $n\geqslant 2$，左端的绝对值总是常数，但符号是交替变化的.

16. $m/n<u/v\Rightarrow mv<nv\Rightarrow mv+amn<nu+amn$

$$\Rightarrow m(an+v)<n(am+u).$$

这个结论也可以通过考虑以 $(0,0)$，(an,am)，$(an+v,am+u)$ 和 (v,u) 为顶点的平行四边形而得到.

17. $\dfrac{p_n}{q_n}=\dfrac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}}\Rightarrow\dfrac{p_n}{q_n}$ 在 $\dfrac{p_{n-1}}{q_{n-1}}$ 与 $\dfrac{p_{n-2}}{q_{n-2}}$ 之间

(由问题 16).

将问题 15 (iii)中等式的两端除以 $q_n q_{n-1}$,即可得到问题中给出的等式.因为 q_i 都是正整数,所以当 n 是偶数时,$p_n/q_n > p_{n-1}/q_{n-1}$.于是 $p_{2n}/q_{2n} > p_{2n-1}/q_{2n-1}$,而 p_{2n+1}/q_{2n+1} 则在它们之间.

此外,p_{2n+2}/q_{2n+2} 在 p_{2n+1}/q_{2n+1} 与 p_{2n}/q_{2n} 之间,因此 $[p_{2n+1}/q_{2n+1}, p_{2n+2}/q_{2n+2}]$ 套在 $[p_{2n-1}/q_{2n-1}, p_{2n}/q_{2n}]$ 中,所以每个奇数项小于任何偶数项.

18. $\frac{1}{1}, \frac{4}{3}, \frac{5}{4}, \frac{14}{11}, \frac{61}{48}$.

$61 \cdot 11 - 48 \cdot 14 = -1$.

$[1, 3, 1, 2, 3] = \frac{47}{37}$.

$61 \cdot 37 - 48 \cdot 47 = 1$.

若 $61x - 48y = 61a - 48b$,则 $61(x-a) = 48(y-b)$,从而 $x \equiv a \pmod{48}$,$y = b \pmod{61}$.

19. $\frac{168}{73} = [2, 3, 3, 7] = [2, 3, 3, 6, 1]$.

$[2, 3, 3] = \frac{23}{10}$. $\quad 168 \cdot 10 - 73 \cdot 23 = 1$.

$[2, 3, 3, 6] = \frac{145}{63}$. $\quad 168 \cdot 63 - 73 \cdot 145 = -1$.

20. $96 = 3 \cdot 25 + 21$,

$25 = 1 \cdot 21 + 4$,

$21 = 5 \cdot 4 + 1$,

$4 = 4 \cdot 1$.

$\frac{217}{96} = [2, 3, 1, 5, 4]$.

21. 由除法算式(问题 1.19),

$$a = bq + r_1 \quad , \quad 0 \leqslant r_1 < b \quad .$$

令 $q = a_1$，则

$$\frac{a}{b} = a_1 + r_1/b = a_1 + \frac{1}{b/r_1} \quad ,（若 r_1 \neq 0）.$$

又由除法算式，

$$b = r_1 q' + r_2 \quad , \quad 0 \leqslant r_2 < r_1 \ .$$

令 $q' = a_2$，则

$$b/r_1 = a_2 + r_2/r_1 = a_2 + \frac{1}{r_1/r_2} \quad ,（若 r_2 \neq 0）.$$

再利用除法算式，$r_1 = r_2 q'' - r_3$，$0 \leqslant r_3 < r_2$．再令 $q'' = a_3$．

由于 $r_1, r_2, r_3, \cdots$ 是减小的非负整数列，所以对某个 n 有 $r_n = 0$，因而

$$a/b = [a_1, a_2, \cdots, a_n] \ .$$

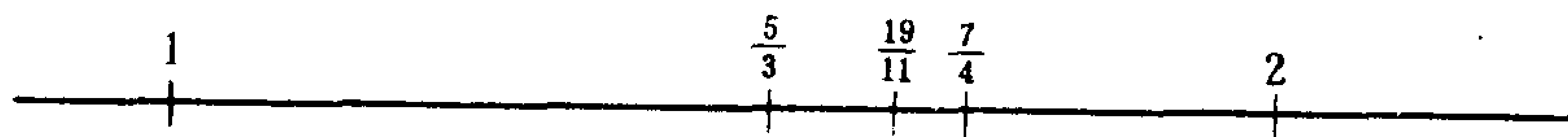
这样，每个正有理数对应着一个有限项简单连分数．若允许 a_1 取负值，则有理数就都可以用有限项简单连分数表示．

22．本题结果表明，若不计最后一项的数字，则有理数的连分数展开式是唯一的．

23．$\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, \cdots]$．

$[1] = 1$， $[1, 1] = 2$， $[1, 1, 2] = \dfrac{5}{3}$， $[1, 1, 2, 1] = \dfrac{7}{4}$，

$[1, 1, 2, 1, 2] = \dfrac{19}{11}$．



若构造渐近分数的过程是有限的，则 $\sqrt{3}$ 将是有理数．反之亦是．

24． $x = a_1 + \dfrac{1}{x_2}$，但 $[x] = a_1$，而且因为 x 是无理数，所以

$0<x-[x]<1$，于是 $0<\dfrac{1}{x_2}<1$.

$x_2=a_2+\dfrac{1}{x_3}$，但 $[x_2]=a_2$，而且因为 x_2 是无理数，所以 $0<x_2-[x_2]<1$.

若 $1<x_n$，则 $1\leqslant[x_n]=a_n$.

若 $x=[a_1,a_2,\cdots,a_{n-1},x_n]$，则由问题 13 得到

$$x=\frac{x_n p_{n-1}+p_{n-2}}{x_n q_{n-1}+q_{n-2}}.$$

因为

$$x=[a_1,a_2,\cdots,a_n,a_{n+1},x_{n+2}]=\frac{x_{n+2}p_{n+1}+p_n}{x_{n+2}q_{n+1}+q_n},$$

所以 x 在 p_{n+1}/q_{n+1} 与 p_n/q_n 之间．但是

$$\left|\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}\right|=\frac{1}{q_n q_{n+1}},$$

所以 $\left|x-\dfrac{p_n}{q_n}\right|<\dfrac{1}{q_n q_{n+1}}$.

25．显然 $c_{2n-1}<c_{2n}$，但是 c_{2n+1} 在这二数之间，所以 $c_{2n-1}<c_{2n+1}$，从而奇数项渐近分数列是单调增加的．类似地可知偶数项渐近分数列是单调减小的．每个偶数项渐近分数是所有奇数项渐近分数的上界，每个奇数项渐近分数是所有偶数项渐近分数的下界．因为，若不是这样，那么，例如就有某两个 m 和 n，使 $c_{2m}<c_{2n+1}$．若 $m>n$，则 $c_{2m+1}<c_{2m}<c_{2n+1}$，这与奇数项渐近分数列的单调增加性矛盾．若 $m\leqslant n$，则 $c_{2m}<c_{2n+1}<c_{2n+2}$，这与偶数项渐近分数列的单调减小性矛盾．

因为 $|c_{2n+1}-c_{2n}|=1/q_{2n+1}q_{2n}$，所以两个数列的项之间的距离趋于零．

$$c_3 < \alpha < c_2 \Rightarrow a_2 < \frac{1}{\alpha - a_1} < a_2 + \frac{1}{a_3}$$

$$\Rightarrow a_2 = \left[\frac{1}{\alpha - a_1} \right], \text{等等}.$$

这些论证建立了无理数集合与所有正整数列(第一项可以是任意整数)集合之间的一一对应，从而使无限简单连分数有了明确的意义.

26. 由 $\alpha = 1 + \frac{1}{\alpha}$ 得到 $\alpha^2 = \alpha + 1$. 因为 $\alpha > 0$，所以

$$\alpha = (1 + \sqrt{5})/2.$$

27. 由 $\alpha = 2 + \frac{1}{\alpha}$ 得到 $\alpha^2 = 2\alpha + 1$. 因为 $\alpha > 0$，所以

$$\alpha = 1 + \sqrt{2}.$$

28. 由 $\alpha = a + \frac{1}{\alpha}$ 得到 $\alpha^2 = a\alpha + 1$. 因为 $\alpha > 0$，所以

$$\alpha = (a + \sqrt{a^2 + 4})/2.$$

29. 由 $\alpha = 1 + \frac{1}{2 + 1/\alpha} = 1 + \frac{\alpha}{2\alpha + 1}$ 得到 $2\alpha^2 + 2 = 3\alpha + 1$，即是 $2\alpha^2 - 2\alpha - 1 = 0$，所以 $\alpha = \frac{1 + \sqrt{3}}{2}$.

30. 由 $\beta = 2 + \frac{1}{1 + 1/\beta} = 2 + \frac{\beta}{\beta + 1}$ 得到 $\beta^2 + \beta = 3\beta + 2$，

即是
$$\beta^2 - 2\beta - 2 = 0 . \quad \beta = 1 + \sqrt{3} .$$

$$2\left(-\frac{1}{\beta}\right)^2 - 2\left(-\frac{1}{\beta}\right) - 1 = -\left(\frac{1}{\beta^2}\right)(\beta^2 - 2\beta - 2) = 0 .$$

31. 由 $\alpha = a + \frac{1}{b + \frac{1}{\alpha}} = a + \frac{\alpha}{b\alpha + 1}$ 得到 $b\alpha^2 - ab\alpha - a = 0$.

这个方程的二根之积是 $-\frac{a}{b}$，因此，一个根 α 是正的，另一个根是负的．

若 $\beta=[\dot{b},\dot{a}]$，则 $a\beta^2-ab\beta-b=0$，β 是这个方程的一个正根．然而 $a-ab\left(\frac{1}{\beta}\right)-b\left(\frac{1}{\beta^2}\right)=0$，所以 $b\left(-\frac{1}{\beta}\right)^2-ab\left(-\frac{1}{\beta}\right)-a=0$，因此 α 与 $-\frac{1}{\beta}$ 都是 $bx^2-abx-a=0$ 的根．

32．由 $\alpha=a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{\alpha}}}=a+\cfrac{1}{b+\cfrac{\alpha}{c\alpha+1}}=a+\frac{c\alpha+1}{(bc+1)\alpha+b}$ 得到 $(bc+1)\alpha^2+(b-a-c-abc)\alpha-ba-1=0$．

若 $\beta=[\dot{c},\dot{b},\dot{a}]$，则 $(ba+1)\beta^2+(b-a-c-abc)\beta-bc-1=0$．于是

$$(bc+1)\left(-\frac{1}{\beta}\right)^2+(b-a-c-abc)\left(-\frac{1}{\beta}\right)-ba-1=0.$$

因此 α 与 $-\frac{1}{\beta}$ 都满足二次方程 $(bc+1)x^2+(b-a-c-abc)x-ba-1=0$．$\alpha$ 与 $-\frac{1}{\beta}$ 是这个方程的不相同的根，因为一个是正的，另一个是负的．

33．由 $\alpha=\frac{\alpha p_n+p_{n-1}}{\alpha q_n+q_{n-1}}$ 得到 $q_n\alpha^2+(q_{n-1}-p_n)\alpha-p_{n-1}=0$．

34．$\frac{p_2}{p_1}=\frac{a_1a_2+1}{a_1}=a_2+\frac{1}{a_1}=[a_2,a_1]$，

$$\frac{p_3}{p_2}=\frac{a_3p_2+p_1}{p_2}=a_3+\frac{1}{p_2/p_1}=[a_3,a_2,a_1].$$

设 $\frac{p_n}{p_{n-1}}=[a_n,a_{n-1},\cdots,a_2,a_1]$，则

$$\frac{p_{n+1}}{p_n}=\frac{a_{n+1}p_n+p_{n-1}}{p_n}=a_{n+1}+\frac{1}{p_n/p_{n-1}}=[a_{n+1},a_n,\cdots,a_2,a_1].$$

35．$\frac{q_2}{q_1}=\frac{a_2}{1}$ 以及 $\frac{q_3}{q_2}=\frac{a_3a_2+1}{a_2}=a_3+\frac{1}{a_2}=[a_3,a_2]$．

设 $q_n/q_{n-1}=[a_n,a_{n-1},\cdots,a_2]$，则

$$\frac{q_{n+1}}{q_n}=\frac{a_{n+1}q_n+q_{n-1}}{q_n}=a_{n+1}+\frac{1}{q_n/q_{n-1}}=[a_{n+1},a_n,\cdots,a_2].$$

36．α 的前 n 个渐近分数是 p_i/q_i $(i\leqslant n)$，所以

$$\alpha=\frac{\alpha p_n+p_{n-1}}{\alpha q_n+q_{n-1}}.$$

β 的第 $n-1$ 个与第 n 个渐近分数分别是 q_n/q_{n-1} 与 p_n/p_{n-1}，所以

$$\beta=\frac{\beta p_n+q_n}{\beta p_{n-1}+q_{n-1}}.$$

$$q_n\alpha^2+(q_{n-1}-p_n)\alpha-p_{n-1}=0.$$

$$p_{n-1}\beta^2+(q_{n-1}-p_n)\beta-q_n=0.$$

37．$q_n\left(-\frac{1}{\beta}\right)^2-(q_{n-1}-p_n)\left(-\frac{1}{\beta}\right)-p_{n-1}=0$．

因为 $\alpha>a_1$，且 $\beta>a_n$，所以 $\alpha>1$ 而且 $-1<-\frac{1}{\beta}<0$．

38．设 $x=1+\sqrt{2}$，则 $(x-1)^2=2$，$x^2-2x-1=0$．

另一个根是 $1-\sqrt{2}$．若 $1+\sqrt{2}$ 是某个二次方程的根，则这个方程必定是 $(x-1-\sqrt{2})(x-\alpha)=0$ 乘以某数．由于是整系数，所以 $\alpha+1+\sqrt{2}$ 与 $\alpha(1+\sqrt{2})$ 都是整数．设 $\alpha+1+\sqrt{2}$

等于整数 a，则 $\alpha=a-1-\sqrt{2}$ ，$\alpha(1+\sqrt{2})=a-3+(a-2)\sqrt{2}$.所以 $a=2$ ，$\alpha=1-\sqrt{2}$.

39．设 $x=\frac{m}{n}+\frac{r}{s}\sqrt{2}$ ，其中 m,n,r,s 都是整数，而且 r,n,s 都不为零，则由 $\left(x-\frac{m}{n}\right)^2=2\frac{r^2}{s^2}$ 可得到所需要的方程.

40．若 $b\neq0$，那么 $\sqrt{2}=-\frac{a}{b}$ 就成了有理数.若 $b=0$，则 $a=0$，结论是显然的.$(a-c)+(b-d)\sqrt{2}=0$.

41．多数结果可直接从有理数对这些运算的封闭性得到.

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\frac{ac-2bd+(bc-ad)\sqrt{2}}{c^2-2d^2};$$

只要 c 和 d 不同时为 0，这就是 $\mathbf{Q}(\sqrt{2})$ 中的数.

42．设 α 与 $a+b\sqrt{2}$ 是方程 $px^2+qx+r=0$ 的根，则

$$p(x-\alpha)(x-a-b\sqrt{2})=px^2+qx+r.$$

因此

$$\alpha+a+b\sqrt{2}=-\frac{q}{p}\ 且\ \alpha(a+b\sqrt{2})=\frac{r}{p}.$$

根据问题 40，由第一个等式得到 $\alpha=c-b\sqrt{2}$ 对某个有理数 c 成立，而由第二个等式得到 $c=a$.

43．$(a-b\sqrt{2})+(c-d\sqrt{2})=(a+c)-(b+d)\sqrt{2}$.

$$(a-b\sqrt{2})(c-d\sqrt{2})=(ac+2bd)-(ad+bc)\sqrt{2}.$$

$$\frac{1}{a-b\sqrt{2}}=\frac{a+b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}+\frac{b}{a^2-2b^2}\sqrt{2}.$$

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}.$$

44．是，$\sqrt{d}$ 的无理性是关键．

45．$\alpha=\alpha_2=1+\sqrt{2}>1$．因为 $-2<-\sqrt{2}<-1$，所以

$$-1<1-\sqrt{2}<0.$$

46．$\beta_2=\frac{1}{3}(2+\sqrt{7})$．因为 $2<\sqrt{7}<3$，所以 $-1<2-\sqrt{7}<0$，$-1<\frac{1}{3}(2-\sqrt{7})<0$．由 $(\beta-2)^2=7$ 得到 $\beta^2-4\beta-3=0$；判别式是 $4^2-4(-3)\cdot 1=28$．

由 $(3\beta_2-2)^2=7$ 得到 $9\beta_2^2-12\beta_2-3=0$ 即 $3\beta_2^2-4\beta_2-1=0$；判别式等于28．

47．若 α_2 是有理数，则由于 $[\alpha]$ 是整数，α 就成了有理数．由问题 41 与问题 44，α_2 属于 $\mathbf{Q}(\sqrt{d})$．

因为 α 是无理数，所以 $0<\alpha-[\alpha]<1$，$1<1/(\alpha-[\alpha])=\alpha_2$．

$$-1<\overline{\alpha}<0 \Rightarrow -1<[\alpha]+1/\overline{\alpha}_2<0,\ (\text{由问题 43 与问题 44})$$

$$\Rightarrow -1-[\alpha]<1/\overline{\alpha}_2<-[\alpha],$$

$$\Rightarrow 0>\frac{-1}{1+[\alpha]}>\overline{\alpha}_2>-\frac{1}{[\alpha]}>-1,$$ （因为 $[\alpha]\geqslant 1$）．

48．将 $\alpha=n+\frac{1}{\alpha_2}$ 代入 $a\alpha^2+b\alpha+c=0$，得到

$$(an^2+bn+c)\alpha_2^2+(2an+b)\alpha_2+a=0$$

及

$$(2an+b)^2-4a(an^2+bn+c)=b^2-4ac.$$

这类似于在二次型 $ax^2+bxy+cy^2$ 中用 $(nx+y,x)$ 替换 (x,y)．

49．$p=1$，$q=1$ 或 2．

50．$p=3$，$q=1,2,3,4,5,6$；

$p=2$，$q=2,3,4,5$；

$p=1$，$q=3,4$．

51．因为 $(p+\sqrt{d})/q>1>0>(p-\sqrt{d})/q$，所以 q 是正的．因为 $|p+\sqrt{d}|>|p-\sqrt{d}|$，所以 p 是正的．因为 $p+\sqrt{d}>0>p-\sqrt{d}$，所以 $\sqrt{d}>-p>-\sqrt{d}$，从而 $\sqrt{d}>p$．因为

$p+\sqrt{d}>q$ 且 $\sqrt{d}>p$，所以 $2\sqrt{d}>p$．这样，数对 (p,q)的个数只能是小于 $2d$．

52．设 $a\alpha^2+b\alpha+c=0$，则 $\alpha=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$．

不妨设 $a>0$ 且 a,b,c 无公约数．这样，由于 $\alpha>\overline{\alpha}$，根式应取正号，而且，与上题一样，得到 $-b>0$．因此，$\alpha=(p+\sqrt{d})/q$，其中p,q 是正整数．

53．(i)，(ii)，(iii) 可由问题 48 得到．

(vi) $a_n+\dfrac{1}{\alpha_{n+1}}=\alpha_n=\alpha_m=a_m+1/\alpha_{m+1}$，所以 $a_n=a_m$ 且 $\alpha_{n+1}=\alpha_{m+1}$．

(vii) 由 $0>\overline{\alpha}_n>-1$ 推出 $-1/\overline{\alpha}_n>1$．

(viii) 由问题 43 及 $\alpha_{n-1}=a_{n-1}+\dfrac{1}{\alpha_n}$ 得出．

将此处结果与问题 33 及问题 37 做比较．

现在我们知道，每个纯循环连分数表示一个二次无理数 α，$\alpha>1$ 且 $0>\overline{\alpha}>-1$．

54．$n=1$，$1+\sqrt{2}=[2,2,2,\cdots]$，$\sqrt{2}=[1,\dot{2}]$．

55．$1+\sqrt{3}=[2,1,\dot{2},\dot{1}]$，$\sqrt{3}=[1,\dot{1},\dot{2}]$．

$2+\sqrt{5}=[4,4,\dot{4}]$，$\sqrt{5}=[2,\dot{4}]$．

$2+\sqrt{6}=[4,2,\dot{4},\dot{2}]$，$\sqrt{6}=[2,\dot{2},\dot{4}]$．

$2+\sqrt{7}=[4,\dot{1},1,1,\dot{4}]$，$\sqrt{7}=[2,\dot{1},1,1,\dot{4}]$．

56．是的，因为若 $\alpha=[\sqrt{d}]+\sqrt{d}$，则 $\alpha>1$，$0>\overline{\alpha}>-1$．

58．$0>5-\sqrt{33}>-1$，因为 $6>\sqrt{33}>5$，所以 $a_1=10$．

若$\alpha=5+\sqrt{33}$，则 $1/(\sqrt{33}-5)=-1/\overline{\alpha}$．二次无理数 α 与 $\overline{\alpha}$ 满足同一个整系数二次方程．

59．$[\sqrt{d}]+\sqrt{d}$ 是纯循环连分数，所以 $a_1=[\sqrt{d}]$，$a_n=2[\sqrt{d}]$．$a_2=a_{n-1}$，$a_3=a_{n-2}$，等等．

60．利用问题 13．

62．$15^2-14\cdot4^2=1$．

63．渐近分数是 $\frac{3}{1}$，$\frac{4}{1}$，$\frac{7}{2}$，$\frac{11}{3}$，$\frac{18}{5}$，$\frac{119}{33}$，$\frac{137}{38}$，$\frac{256}{71}$，$\frac{393}{109}$，$\frac{649}{180}$．$18^2-13\cdot5^2=-1$，$649^2-13\cdot180^2=1$．

65．若 $\sqrt{d}$ 的最小周期是偶数，则问题 61 给出确定的答案．若 $\sqrt{d}$ 的最小周期是奇数，取 n 等于最小周期长度的二倍，则仍可用问题 61．

66．
$$
\begin{aligned}
a^2-2b^2=1 &\Rightarrow (a+b\sqrt{2})(a-b\sqrt{2})=1\\
&\Rightarrow (a+b\sqrt{2})^2(a-b\sqrt{2})^2=1^2\\
&\Rightarrow (a^2+2b^2+2ab\sqrt{2})(a^2+2b^2-2ab\sqrt{2})\\
&\quad =1\\
&\Rightarrow (a^2+2b^2)^2-2(2ab)^2=1.
\end{aligned}
$$

由于 $a^2+2b^2>a$，所以这个解与最初的解不同，因此，这个过程可以反复进行，但不出现重复．

67．由乘积得到 $1\leqslant(x+y\sqrt{2})(a-b\sqrt{2})^n<a+b\sqrt{2}$．但是若 $x^2-2y^2=1$ 且 $c^2-2d^2=1$，则 $(x+y\sqrt{2})(c+d\sqrt{2})$ 也是一个解．所以 $(x+y\sqrt{2})(a-b\sqrt{2})^n$ 是一个解，根据定义，它等于1．

68．推广问题 67 的论证．

69．若 $x+y\sqrt{d}=(a+b\sqrt{d})^n$，则由问题 43 的推广，可知 $x-y\sqrt{d}=(a-b\sqrt{d})^n$．因此一切解都是这种形式．注意 $x=\overline{x}$ 且 $y=\overline{y}$．

70．$x=\frac{1}{2}[(3+2\sqrt{2})^n+(3-2\sqrt{2})^n]$，$y=\frac{1}{2\sqrt{2}}[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n]$．$(x+4y+3)^2-2y^2=1$．

71．$9^2-5\cdot4^2=1$，$18^2-5\cdot8^2=4$，$3^2-5\cdot1^2=4$．

$(a+b\sqrt{5})(a-b\sqrt{5})[(c+d\sqrt{5})(c-d\sqrt{5})]=16$，所以

$$[(a+b\sqrt{5})(c+d\sqrt{5})][(a-b\sqrt{5})(c-d\sqrt{5})]=16,$$
$$2(p+q\sqrt{5})\cdot 2(p-q\sqrt{5})=16.$$

$a^2-5b^2=4 \Rightarrow a \equiv b \pmod 2$. 于是$ac+5bd \equiv 6ac \equiv 0 \pmod 2$. 因此$p$是整数，并且由$p^2-5q^2=4$知道$q$也是整数.

$$2\left(\frac{3+\sqrt{5}}{2}\right)\left(\frac{3+\sqrt{5}}{2}\right)=7+3\sqrt{5},$$

$$2\left(\frac{3+\sqrt{5}}{2}\right)\left(\frac{7+3\sqrt{5}}{2}\right)=18+8\sqrt{5}.$$

72. $n=2$时，$n+\alpha$是纯循环连分数.

73. 若存在这样的n，则$n+\alpha$就是纯循环的，这不可能，所以不存在这样的n.

74. $\frac{1}{2}(3+\sqrt{12})>3, 0>\frac{1}{2}(3-\sqrt{12})>-1$；纯循环的.

$2+\sqrt{5}>4, 0>2-\sqrt{5}>-1$；$3+\sqrt{5}$从第二项开始是循环的.

$\overline{3-\sqrt{5}}>3-\sqrt{5}$；都不是.

若$n+\frac{1}{4}\sqrt{3}>1$，则$n-\frac{1}{4}\sqrt{3}>0$；都不是.

75. $\frac{1}{4}\sqrt{3}<1$，所以不是纯循环的.

$n+\frac{1}{4}\sqrt{3}>1 \Rightarrow n \geqslant 1 \Rightarrow n-\frac{1}{4}\sqrt{3}>0$，所以不可能从第二项开始是循环的.

76. 当$n \to \infty$时，$\frac{p_{n-1}}{q_{n-1}}$与$\frac{p_{n-2}}{q_{n-2}}$都趋于α，所以$\overline{\alpha}_n$趋于$-\frac{q_{n-2}}{q_{n-1}}$. 但q_n是递增的无界正整数列，所以$0>-\frac{q_{n-2}}{q_{n-1}}>-1$.

当 $n>1$ 时，$\alpha_n>1$，所以对充分大的 n，$\alpha_n>1$，$0>\overline{\alpha_n}>-1$.

77．每一个混循环连分数都具有形式

$$[a_1, a_2, \cdots, a_{n-1}, \alpha_n],$$

其中 α_n 是纯循环的连分数．设 $\alpha=[a_1, a_2, \cdots, a_{n-1}, \alpha_n]$，则由问题 13，

$$\alpha=\frac{\alpha_n p_{n-1}+p_{n-2}}{\alpha_n q_{n-1}+q_{n-2}}.$$

由问题 33，α_n 是二次无理数，所以 α 属于 $\mathbf{Q}(\sqrt{d})$，而且它的连分数不是有限的．因此，根据问题 21 知道 α 是无理数．

78．$p_n/q_n=\frac{1}{1}, \frac{4}{3}, \frac{9}{7}, \frac{31}{24}$.

$$\alpha_n=\frac{1}{3}(0+\sqrt{15}), \frac{1}{2}(3+\sqrt{15}),$$
$$\frac{1}{3}(3+\sqrt{15}), \frac{1}{2}(3+\sqrt{15}).$$

$3p^2-5q_n^2=-2, 3, -2, 3$.

$B_n=3, 2, 3, 2$.

79．$$\frac{a}{b}+\frac{c}{d}\sqrt{15}=\frac{ad\pm\sqrt{15b^2c^2}}{bd};$$

$$\frac{A+\sqrt{N}}{B}=\frac{AB+\sqrt{NB^2}}{B^2};$$

$$B^2 \mid NB^2-(AB)^2;\quad \frac{A-\sqrt{N}}{B}=\frac{(-A)+\sqrt{N}}{(-B)}.$$

$$\beta=\frac{1}{\alpha-n}=\frac{B}{A+\sqrt{N}-nB}=\frac{B(-A+nB+\sqrt{N})}{N-(A-nB)^2}.$$

因为 $B \mid N-A^2$，所以 $B \mid N-A^2+2nB-B^2$．取 $D=[N-(A-nB)^2]/B$，则显然 $D \mid N-(A-nB)^2$．因此，令 $C=-A+nB$，则

可得到 β 的标准形.

比较有理部分，得到

$$5q_{n-1}=A_np_{n-1}+B_np_{n-2}.$$

比较无理部分，得到

$$3p_{n-1}=A_nq_{n-1}+B_nq_{n-2}.$$

第二个等式乘以 p_{n-1} 减去第一个等式乘以 q_{n-1}，即可得到结论.

80. $(\pm 1,0)$，$(\pm 4,\pm 3)$在以 $y=\pm\sqrt{\frac{3}{5}}x$ 为渐近线的双曲线上. $(pa+5kb,3ka+pb)$在曲线 $3x^2-5y^2=3$ 上的充要条件，是

$$3(pa+5kb)^2-5(3ka+pb)^2=3,$$

即

$$(3p^2-45k^2)a^2-(5p^2-75k^2)b^2=3,$$

即

$$3a^2-5b^2=3.$$

是么模变换.

矩阵之积为 $\begin{pmatrix}3 & 0\\ 0 & -5\end{pmatrix}$，所以这个变换使二次型保持不变，因而是这个型的一个自守变换. 对于适当的乘法，这个对应关系是一个同构. $p^2-15k^2=1$ 的解都是最小解的幂；它们构成了一个具有乘法的无限循环群.

81. 若 $p^2-abk^2=1$，则

$$\begin{pmatrix}p & ak\\ bk & p\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & -b\end{pmatrix}\begin{pmatrix}p & bk\\ ak & p\end{pmatrix}=\begin{pmatrix}a & 0\\ 0 & -b\end{pmatrix},$$

因此 $(x,y)\to(x,y)\begin{pmatrix}p & ak\\ bk & p\end{pmatrix}$ 是 ax^2-by^2 的一个自守变换. 具有矩阵乘法的形如 $\begin{pmatrix}p & ak\\ bk & p\end{pmatrix}$ 的矩阵的集合，与具有乘法的所有形如 $p+k\sqrt{ab}$ 的数的集合是同构的，所以这种矩阵的每个幂也

是一个自守变换.

82. $p^2=s^2$,所以$p=\pm s$.若$p=s$,则由(iv),可设$3r=5q=15k$,得到第一种自守变换形式.若$p=-s$,则由(iv),可设$3r=-5q=-15k$,得到第二种自守变换形式.

历史注记

Pythagoras学派在公元前约550年就已经知道平方根的无理性了.在Euclid的除法算式(公元前约300年)中,蕴含了有限连分数的概念.约在公元500年,印度数学家Aryabhata曾使用连分数去解方程$ax+by=y$.某些二次无理数的循环连分数,在16世纪已经知道了.1665年,John Wallis在他出版的书中使用了"连分数"这个名词.1685年,他又指出如何使用连分数去得到某些无理数的好的逼近.我们这里所用到的连分数理论的绝大部分,在1795年出版并且附有Lagrange写的附录的L.Euler的著作Algebra中都可找到.

1657年,Fermat宣布当d是非平方数时,方程$x^2-dy^2=1$有无限多个解.Euler错误地认为Wallis的书中所给出的一个方法是属于Fermat的同代人John Pell,这个方程的惯用名称就是从这个错误而来的."Fermat方程"应该是这个方程的更合适的名称.1765年,Euler利用$\sqrt{d}$的连分数得到方程$x^2-dy^2=1$的一个解,但这个方程的全部解则是Lagrange所确定的(1769,1770).1842年,G.P.L.Dirichlet根据对Gauss整数环上的二次型的分析,确定了不定型的自守变换.

第十一章　无理数的有理逼近

自然逼近

1. 哪个整数离 $\sqrt{2}$ 最近? 哪个整数离 $\sqrt{3}$ 最近?

2. 设 α 是实数、那么对于 $\alpha-[\alpha]$ 的值能有什么估计? 是否必有整数 n，使得 $|\alpha-n|\leqslant \frac{1}{2}$？若 α 是无理数，这个不等式能否改进?

3. 在数轴上标出所有整点 n 以及它们的中点 $n+\frac{1}{2}$. 数轴上的任一点与这些点的最近距离能有多么大?

求整数 m 与 k 使得 $\left|\sqrt{2}-\frac{1}{2}m\right|<\frac{1}{4}$，$\left|\sqrt{5}-\frac{1}{2}k\right|<\frac{1}{4}$.

对于任意实数 α，是否必有整数 m，使得 $\left|\alpha-\frac{1}{2}m\right|<\frac{1}{4}$？

4. 对于所有整数 n，在数轴上标出点 n，$n+\frac{1}{3}$，$n+\frac{2}{3}$. 数轴上任一点与这些点的最近距离能有多么大?

求整数 m 与 k，使得

$$\left|\sqrt{2}-\frac{1}{3}m\right|<\frac{1}{6}，\left|\sqrt{3}-\frac{1}{3}k\right|<\frac{1}{6}.$$

对于任意的无理数α，是否必有整数m，使得$\left|\alpha-\frac{1}{3}m\right|<\frac{1}{6}$？

5. 对于任意的无理数α，是否必有整数m，使得$\left|\alpha-\frac{1}{3}m\right|<\frac{1}{9}$？区间$[1,2]$中，与点$1$，$\frac{4}{3}$，$\frac{5}{3}$或$2$的距离小于$\frac{1}{9}$的那些点所构成的区间的总长度是多少?

求实数α，使得对于任意整数m有$\left|\alpha-\frac{1}{3}m\right|>\frac{1}{9}$.

6. 设α是无理数，q是给定的正整数，是否总存在整数p，使得$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q}$？是否总有整数$p$，使得$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}$？

7. 用袖珍计算器计算$n\sqrt{2}-[n\sqrt{2}]$ $(n=1,2,\cdots,11)$到二位小数. 这十一个数为什么两两不相等? 为什么对任意整数k，它们都不取值$\frac{1}{10}k$？

证明这十一个数中的每一个都恰好属于开区间$\left(0,\frac{1}{10}\right)$，$\left(\frac{1}{10},\frac{2}{10}\right)$，…，$\left(\frac{9}{10},1\right)$中的一个.

在这些数中，选取属于同一开区间的两个数，并求整数p，q，使得$|q\sqrt{2}-p|<\frac{1}{10}$.

8. 用问题7的方法，求整数p，q，使得$|q\sqrt{3}-p|<\frac{1}{10}$. 这个方法能否保证$q\leqslant 10$？

9. 推广问题7与8的方法证明：对于任意的无理数α和任意给定的正整数n，可以找到整数p与q，使得$|q\alpha-p|<\frac{1}{n}$且

$0<q\leqslant n$.

10. 利用问题 9 证明，对于任意的无理数 α 及任意给定的正整数 n，可以找到整数 p，q，使得 $\left|\alpha-\dfrac{p}{q}\right|<\dfrac{1}{q^2}$ 且 $0<q\leqslant n$.

Farey 数 列

11. 为了考察分母不超过 n 的有理数的密集情况，我们来研究问题 8.13 中的 Farey 数列 F_n：

$$F_5\quad \frac{0}{1}\quad \frac{1}{5}\ \frac{1}{4}\quad \frac{1}{3}\ \frac{2}{5}\quad \frac{1}{2}\quad \frac{3}{5}\ \frac{2}{3}\quad \frac{3}{4}\ \frac{4}{5}\quad \frac{1}{1}$$

$$F_6\quad \frac{0}{1}\quad \frac{1}{6}\ \frac{1}{5}\ \frac{1}{4}\quad \frac{1}{3}\ \frac{2}{5}\quad \frac{1}{2}\quad \frac{3}{5}\ \frac{2}{3}\quad \frac{3}{4}\ \frac{4}{5}\ \frac{5}{6}\quad \frac{1}{1}$$

$$F_7\quad \frac{0}{1}\ \frac{1}{7}\ \frac{1}{6}\ \frac{1}{5}\ \frac{1}{4}\ \frac{2}{7}\ \frac{1}{3}\ \frac{2}{5}\ \frac{3}{7}\ \frac{1}{2}\ \frac{4}{7}\ \frac{3}{5}\ \frac{2}{3}\ \frac{5}{7}\ \frac{3}{4}\ \frac{4}{5}\ \frac{5}{6}\ \frac{6}{7}\ \frac{1}{1}$$

将 F_5 中的项数与 $1+\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(5)$ 比较.

试猜测 F_n 中的项数.

证明你的猜测.

12. 设 $\dfrac{a}{b}$ 与 $\dfrac{c}{d}$ 是一个 Farey 数列中的相邻项，求以 $(0,0)$，(b,a)，(d,c) 为顶点的三角形面积. 参见问题 8.12.

13. 设 $\dfrac{a}{b}$，$\dfrac{c}{d}$，$\dfrac{e}{f}$ 是一个 Farey 数列中依次相邻的三项，令 $O=(0,0)$，$A=(b,a)$，$C=(d,c)$ 及 $E=(f,e)$，求三角形 OCA 与 OCE 的面积. 设 H 与 K 分别是由 A 与 E 到 OC 的垂线的垂足，为什么 $AH=EK$？

在关于 HK 的中点作半周旋转之后，O，A 及 E 的像的坐标是什么？推导 $\frac{c}{d}=\frac{a+e}{b+f}$．将本方法与问题 8.14 作比较．

14．设 $\frac{a}{b}$ 与 $\frac{c}{d}$ 是 Farey 数列 F_n 中的相邻两项，证明三角形 $(0,0)$，(b,a)，$(b+d,a+c)$ 与 $(0,0)$，(d,c)，$(b+d,a+c)$ 的面积都是 $\frac{1}{2}$，并求最短的 Farey 数列，使得 $\frac{a}{b}$，$\frac{a+c}{b+d}$，$\frac{c}{d}$ 为其依次相邻的三项．

为什么一定是 $b+d>n$？

15．设 a, b, c, d 是正实数且 $\frac{a}{b}<\frac{c}{d}$，用几何方法证明：

$$\frac{a}{b}<\frac{a+c}{b+d}<\frac{c}{d},$$

而且，对于任意的正数 u, v，有

$$\frac{a}{b}<\frac{au+c}{bu+d}<\frac{c}{d}, \quad \frac{a}{b}<\frac{a+cv}{b+dv}<\frac{c}{d}.$$

将你的证明与问题 10.16 作比较．

16．给出下述结论的代数证明或几何证明：对于任意的正实数 a,b,c,d,u,v，若 $\frac{a}{b}<\frac{c}{d}$，则 $\frac{a}{b}<\frac{au+cv}{bu+dv}<\frac{c}{d}$．

设 a,b,c,d 是正整数，那么，在 $\frac{a}{b}$ 与 $\frac{c}{d}$ 之间的有理数是否都是 $\frac{au+cv}{bu+dv}$ 的形式，其中 u,v 是适当选取的整数？

17．若 $\frac{a}{b}$ 与 $\frac{c}{d}$ 是 Farey 数列 F_n 中的相邻两项，则称 $\frac{a+c}{b+d}$ 是它们的中项．

考察 Farey 数列 F_n，F_{n-1}，$F_{n+2}\cdots$，证明第一个出现在 $\frac{a}{b}$ 与 $\frac{c}{d}$ 之间的分数是它们的中项，并且

$$\left|\frac{a+c}{b+d}-\frac{a}{b}\right|\leqslant\frac{1}{b(n+1)},\left|\frac{c}{d}-\frac{a+c}{b+d}\right|\leqslant\frac{1}{d(n+1)}.$$

18. $\frac{1}{\sqrt{2}}$ 分别落在 F_2，F_3，F_4，F_5，F_6，F_7 的哪两项中间？

对每一种情况，确定 $\frac{1}{\sqrt{2}}$ 比这两个项的中项大还是小？

对于 $n=2,3,4,5,6,7$，求有理数 $\frac{a}{b}$，使得 $\left|\frac{1}{\sqrt{2}}-\frac{a}{b}\right|\leqslant\frac{1}{b(n+1)}$，且 $b\leqslant n$。

19. 设 α 是 0 与 1 之间的任意实数，是否一定存在整数 a，b，使得 $\left|\alpha-\frac{a}{b}\right|\leqslant\frac{1}{8b}$，且 $b\leqslant 7$？

20. 对于给定的正整数 n 及 $0\leqslant\alpha\leqslant 1$，为什么存在整数 a，b，使得 $\left|\alpha-\frac{a}{b}\right|\leqslant\frac{1}{b(n+1)}$ 并且 $b\leqslant n$？

21. 说明上题中的条件 $0\leqslant\alpha\leqslant 1$ 可以去掉的原因.

22. 利用问题 20 给出问题 10 的另一个证明.

Hurwitz 定理

到目前为止，我们已经用两种不同的方法证明了：对于任意无理数 α，存在整数 p，q，使得 $\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}$。我们将证明满

足这个条件的有理数 $\frac{p}{q}$ 有无限多个，随后，将看到如何利用 α 的连分数的渐近分数求出这些有理数，并改进已有的逼近精确度.

23. 对于正整数 $b=1,2,3,4,5$ 中的哪些数，存在整数 a，使得 $\left|\sqrt{2}-\frac{a}{b}\right|<\frac{1}{b^2}$？

24. 设 α 等于有理数 $\frac{p}{q}$，此处 $\gcd(p,q)=1$，证明对于任何非零整数 a，b（使 $\frac{a}{b}=\frac{p}{q}=\alpha$ 的除外），都有 $|b\alpha-a|\geqslant\frac{1}{q}$.

25. 设 $\left|\alpha-\frac{a}{b}\right|<\frac{1}{b^2}$，且 α 不是有理数，利用问题 20 并适当选取 n，证明可以找到整数 p，q，使得 $\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}$，而且 $\left|\alpha-\frac{p}{q}\right|<\left|\alpha-\frac{a}{b}\right|$. 证明存在无限多对整数 a，b，使得 $\left|\alpha-\frac{a}{b}\right|<\frac{1}{b^2}$.

26. 设 p_{n-1}/q_{n-1} 与 p_n/q_n 是无理数 α 的相邻的渐近分数，利用 α 介于这两个渐近分数之间的事实，证明

$$\left|\alpha-\frac{p_{n-1}}{q_{n-1}}\right|<\frac{1}{q_{n-1}q_n}<\frac{1}{q_{n-1}^2}.$$

27. 对 $n=1,2,\cdots,30$，用计算器计算 $(n\sqrt{2}-[n\sqrt{2}])n$ 的值到三位小数.

将这些数值与 $\left|\sqrt{2}-\frac{p}{q}\right|q^2$ 做比较，其中 $\frac{p}{q}$ 分别取 $\sqrt{2}$ 的前五个渐近分数值.

猜测一个方法，用以寻求使$\left|\sqrt{2}-\frac{p}{q}\right|q^2<\frac{1}{2}$成立的整数$p,q$.

28. 设p_n/q_n及p_{n+1}/q_{n+1}是$\sqrt{2}$的相邻的渐近分数，使得

$$\left|\sqrt{2}-\frac{p_n}{q_n}\right|q_n^2\geqslant\frac{1}{2}\text{ 且}\left|\sqrt{2}-\frac{p_{n+1}}{q_{n+1}}\right|q_{n+1}^2\geqslant\frac{1}{2}.$$

利用问题 10.24 证明.

$$\frac{1}{q_n q_{n+1}}\geqslant\frac{1}{2}\left(\frac{1}{q_n^2}+\frac{1}{q_{n+1}^2}\right).$$

由此推出$0\geqslant(q_n-q_{n+1})^2$，但这是不可能的.

证明存在无限多个有理数$\frac{p}{q}$使得$\left|\sqrt{2}-\frac{p}{q}\right|<\frac{1}{2q^2}$，其中$p$与$q$互素.

29. 对于任意的无理数α，证明它的任何两个相邻的渐近分数中，至少有一个满足不等式$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}$，并由此证明，存在无限多对互素的整数$p, q$满足这个不等式.

30. (i) 设p_{n-1}/q_{n-1}与p_n/q_n是$\sqrt{2}$的相邻的渐近分数，使得

$$\left|\sqrt{2}-\frac{p_{n-1}}{q_{n-1}}\right|q_{n-1}^2\geqslant\frac{1}{\sqrt{5}},\quad\left|\sqrt{2}-\frac{p_n}{q_n}\right|q_n^2\geqslant\frac{1}{\sqrt{5}},$$

利用问题 10.24 证明

$$\frac{1}{q_{n-1}q_n}\geqslant\frac{1}{\sqrt{5}}\left(\frac{1}{q_{n-1}^2}+\frac{1}{q_n^2}\right),$$

并推出

$$\sqrt{5}\geqslant\frac{q_n}{q_{n-1}}+\frac{q_{n-1}}{q_n}.$$

等号为什么不能成立?

(ii) 对于$x>0$画出$y=x+\frac{1}{x}$的草图. 若$y<\sqrt{5}$，x可取

什么值? 证明: 当 $x>1$ 且 $y<\sqrt{5}$ 时, 必有 $x<\frac{1}{2}(\sqrt{5}+1)$, 即 $\frac{1}{x}>\frac{1}{2}(\sqrt{5}-1)$.

(iii) 设 p_{n-1}/q_{n-1}, p_n/q_n 与 p_{n+1}/q_{n+1} 是 $\sqrt{2}$ 的三个相邻的渐近分数, 使得 $|\sqrt{2}-p_i/q_i|q_i^2\geqslant 1/\sqrt{5}$ $(i=n-1, n, n+1)$, 利用(i)与(ii)证明

$$1+\frac{q_{n-1}}{q_n}>\frac{1}{2}(\sqrt{5}+1)>\frac{q_{n+1}}{q_n}.$$

利用在问题 10.13 中得到的 q_{n-1}, q_n 与 q_{n+1} 的关系式, 导出一个矛盾.

31. 对于任意的无理数 α, 证明它的三个相邻的渐近分数中至少有一个满足 $|\alpha-p/q|<1/\sqrt{5}\,q^2$, 并由此证明存在无限多对互素的整数 p, q 满足这个不等式.

(Hruwitz 定理)

在以下两个问题中, 我们将证明, Hurwitz 定理中的 $\sqrt{5}$ 是使这样一个定理成立所能取的最大数值.

32. 求 $\frac{1}{2}(\sqrt{5}+1)$ 的连分数.

33. (i) 设 $\left|\frac{1}{2}(\sqrt{5}+1)-\frac{p}{q}\right|=\frac{1}{cq^2}$, 证明

$$p^2-pq-q^2=1/c^2q^2\pm\sqrt{5}/c.$$

(ii) 对于任意的非零整数 p, q, 证明 $p^2-pq-q^2\neq 0$.

(iii) 设 $c>\sqrt{5}$, 证明

$$-1<\frac{1}{c^2q^2}\pm\frac{\sqrt{5}}{c}<1$$

对于充分大的 q 成立.

(iv) 利用(i)，(ii)，(iii) 证明：若 $c>\sqrt{5}$，则使 $\left|\frac{1}{2}(\sqrt{5}+1)-\frac{p}{q}\right|<\frac{1}{cq^2}$ 成立的有理数 $\frac{p}{q}$ 至多是有限个.

Liouville 定理

直到现在，我们一直致力于寻求无理数的好的有理逼近，以及确定利用相应的连分数的渐近分数所可能达到的逼近精确度. 在本章的余下部分，我们将看到，对于一类特殊的无理数(代数数)，即使是最好的有理逼近也不能达到特别高的精确度.

34. 设 p, q 是正整数，证明 $|p^2/q^2-2|\geqslant \frac{1}{q^2}$.

画出 $y=x^2-2$ 的草图并证明：当 $1\leqslant p/q\leqslant 2$ 时，

$$\frac{|p^2/q^2-2|}{|p/q-\sqrt{2}|}\leqslant\frac{2}{2-\sqrt{2}}.$$

推导 $\left|\frac{p}{q}-\sqrt{2}\right|\geqslant(2-\sqrt{2})/2q^2$.

说明这个不等式当 p/q 不在 1 与 2 之间时也成立的原因. 证明对于一切非零整数 p，q，$|p/q-\sqrt{2}|>1/4q^2$.

35. 对于哪些正整数 p，q，有 $|p/q-\sqrt{2}|<1/q^3$？

对于任意正实数 c，证明使 $|p/q-\sqrt{2}|<c/q^3$ 成立的互素整数对 p，q 至多有有限对.

36. 画出 $y=x^2-3$ 的草图，并利用问题34 的方法证明：对于正整数 p，q，总有 $|p/q-\sqrt{3}|\geqslant(2-\sqrt{3})/q^2>1/5q^2$. 对于任意正实数 c，证明使 $|p/q-\sqrt{3}|<c/q^3$ 成立的互素整数对 p，q 至多有有限对.

37. 画出 $y=x^2-x-1$ 的草图，并证明对于正整数 p, q，总有

$$|p^2/q^2-p/q-1|\geqslant\frac{1}{q^2}.$$

证明

$$\frac{\left|p^2/q^2-p/q-1\right|}{\left|p/q-\frac{1}{2}(\sqrt{5}+1)\right|}\leqslant\frac{2}{3-\sqrt{5}}.$$

推导 $\left|p/q-\frac{1}{2}(\sqrt{5}+1)\right|\geqslant(3-\sqrt{5})/2q^2>\frac{1}{3q^2}$.

38. 证明$\sqrt[3]{2}$是无理数，进而推出：对于任意的正整数p，q，有$|p^3/q^3-2|\geqslant\frac{1}{q^3}$.

画出$y=x^3-2$的草图，并证明当$1\leqslant\frac{p}{q}\leqslant2$时，

$$\left|\frac{p^3/q^3-2}{p/q-\sqrt[3]{2}}\right|\leqslant\frac{6}{2-\sqrt[3]{2}}.$$

推导$|p/q-\sqrt[3]{3}|\geqslant(2-\sqrt[3]{2})/6q^3>\frac{1}{12q^3}$.

说明对于任意的正整数p，q，有$|p/q-\sqrt[3]{2}|>\frac{1}{12q^3}$成立的原因. 证明满足$|p/q-\sqrt[3]{2}|<\frac{1}{q^4}$的互素整数对$p$，$q$至多有有限对，以及，对于任意给定的正实数$c$，满足$|p/q-\sqrt[3]{2}|<\frac{c}{q^4}$的互素整数对$p$，$q$至多有有限对.

39. 证明$\frac{1}{3}(2-\sqrt[3]{2})$是无理数，进而证明它是方程$9x^3-18x^2+12x-2=0$的唯一实根.

利用这个方程没有有理根的事实，证明对于任意的整数p，q，有

$$\left|9\frac{p^3}{q^3}-18\frac{p^2}{q^2}+12\frac{p}{q}-2\right|\geqslant\frac{1}{q^3}.$$

画出$y=9x^3-18x^2+12x-2$当$0<x<1$时的草图，尽量画得仔细一些.

推导

$$\frac{\left|9\frac{p^3}{q^3}-18\frac{p^2}{q^2}+12\frac{p}{q}-2\right|}{\left|p/q-\frac{1}{3}(2-\sqrt[3]{2})\right|}\leqslant\frac{6}{2-\sqrt[3]{2}}\qquad\left(0<\frac{p}{q}<1\right)$$

以及

$$\left|\frac{p}{q}-\frac{1}{3}(2-\sqrt[3]{2})\right|\geqslant(2-\sqrt[3]{2})/6q^3.$$

证明对于一切正整数 p，q，有

$$\left|p/q-\frac{1}{3}(2-\sqrt[3]{2})\right|>\frac{1}{12q^3},$$

进而推出，对于给定的正数 c，使 $\left|\frac{p}{q}-\frac{1}{3}(2-\sqrt[3]{2})\right|<\frac{c}{q^4}$ 成立的互素整数对 p，q 至多有有限对.

40. 设 α 是满足整系数方程

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$$

的无理数，其中 $a_n\neq 0$，并且 α 不再满足任何低次的整系数方程，证明对于任意的正整数 q 与任意整数 p，有

$$\left|a_n\frac{p^n}{q^n}+a_{n-1}\frac{p^{n-1}}{q^{n-1}}+\cdots+a_1\frac{p}{q}+a_0\right|\geqslant\frac{1}{q^n}.$$

这样的数 α 称为n次代数数.

41. 设f 是实的可微函数，α 是它的一个零点，那么由中值定理知道，对于任意的实数 $b\neq\alpha$，必有某个 x 使得 $\frac{f(b)}{b-\alpha}=f'(x)$，此处 x 满足 $\alpha\leqslant x\leqslant b$，或 $b\leqslant x\leqslant\alpha$. 设$|f'(x)|$在闭区间

$\left[\alpha-\frac{1}{2},\alpha+\frac{1}{2}\right]$上的最大值是$A$，证明当$\alpha-\frac{1}{2}\leqslant b\leqslant\alpha+\frac{1}{2}$时，有$|b-\alpha|\geqslant f(b)/A$成立.

42. 设α是$(n\geqslant 2)$次代数数，证明存在正实数A，使得对于一切整数p与一切正整数q，有$|p/q-\alpha|>\frac{1}{Aq^n}$.（Liouville定理）

43. 设$\alpha=\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\frac{1}{10^{4!}}+\cdots$，

即

$$\alpha=\frac{1}{10}+\frac{1}{10^2}+\frac{1}{10^6}+\frac{1}{10^{24}}+\cdots.$$

再设

$\frac{p_1}{q_1}=\frac{1}{10}$，$\frac{p_2}{q_2}=\frac{1}{10}+\frac{1}{10^2}$，$\frac{p_3}{q_3}=\frac{1}{10}+\frac{1}{10^2}+\frac{1}{10^6}$，

以及，一般地，

$$\frac{p_n}{q_n}=\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\cdots+\frac{1}{10^{n!}},$$

其中p_n与q_n互素. 求p_1，q_1，p_2，q_2，p_3，q_3，q_n.

证明

$$0<\alpha-\frac{p_1}{q_1}<\frac{1}{10^2}+\frac{1}{10^3}+\frac{1}{10^4}+\cdots+\frac{1}{10^i}+\cdots=\frac{1}{10^2}\frac{10}{9}$$
$$=\frac{1}{9}\frac{1}{10}<\frac{1}{q_1},$$

$$0<\alpha-\frac{p_2}{q_2}<\frac{1}{10^6}+\frac{1}{10^7}+\frac{1}{10^8}+\cdots=\frac{1}{10^6}\frac{10}{9}=\frac{1}{9}\frac{1}{10^5}$$
$$<\left(\frac{1}{q_2}\right)^2$$

$$0<\alpha-\frac{p_3}{q_3}<\frac{1}{10^{24}}+\frac{1}{10^{25}}+\frac{1}{10^{26}}+\cdots=\frac{1}{10^{24}}\frac{10}{9}=\frac{1}{9}\frac{1}{10^{23}}$$
$$<\left(\frac{1}{q_3}\right)^3$$

以及，最后有

$$0<\alpha-\frac{p_n}{q_n}<\frac{1}{10^{(n+1)!}}+\frac{1}{10^{(n+1)!+1}}+\cdots=\frac{1}{10^{(n+1)!}}\frac{10}{9}$$
$$<\left(\frac{1}{q_n}\right)^n.$$

证明：不存在使问题 42 中的不等式成立的 n 和 A，所以 α 不是代数数.

一个实数若不是代数数，则称为超越数.

注记与答案

参考书见书目：Niven (1961).

1. $\sqrt{2}-1<\frac{1}{2}$, $2-\sqrt{3}<\frac{1}{2}$.

2. $0\leqslant\alpha-[\alpha]<1$. 若 $\frac{1}{2}<\alpha-[\alpha]$，则 $[\alpha]+1-\alpha<\frac{1}{2}$. 若 α 是无理数，则 $\alpha\neq\frac{1}{2}n$ (n 是任意整数)，于是存在整数 n，使得 $|\alpha-n|<\frac{1}{2}$.

3. $\frac{1}{4}$，$\left|\sqrt{2}-\frac{3}{2}\right|<\frac{1}{4}$，$|\sqrt{5}-2|<\frac{1}{4}$. 除去 $\alpha=\frac{n}{4}$

(n 是奇数)的情形.

4. $\frac{1}{6}$，$\left|\sqrt{2}-\frac{4}{3}\right|<\frac{1}{6}$，$\left|\sqrt{3}-\frac{5}{3}\right|<\frac{1}{6}$.

是的，因为对于任何整数 n，$\alpha \neq \frac{n}{6}$.

5. 不是，例如当 $\frac{1}{9}<\alpha<\frac{2}{9}$ 时. $\frac{2}{3}$. 例如 $\frac{3}{18}$.

6. 因为 α 属于某个区间 $\left(\frac{m}{q}, \frac{m+1}{q}\right)$，所以它与某个端点的距离小于 $\frac{1}{2q}$，因此存在 p，使得 $\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q}$. 若 $q>2$，则

$$\left|\frac{2m+1}{2q}-\frac{m}{q}\right|=\frac{1}{2q}>\frac{1}{q^2}.$$

7. 设 $m\neq n$ 但 $n\sqrt{2}-[n\sqrt{2}]=m\sqrt{2}-[m\sqrt{2}]$，则 $\sqrt{2}=([n\sqrt{2}]-[m\sqrt{2}])/(n-m)$就成了有理数. 若 $n\sqrt{2}-[n\sqrt{2}]=\frac{k}{10}$，情况类似.

$\sqrt{2}-[\sqrt{2}]$ 与 $6\sqrt{2}-[6\sqrt{2}]$ 都在 0.4 与 0.5 之间，所以

$$|(6\sqrt{2}-8)-(\sqrt{2}-1)|<\frac{1}{10},\quad |5\sqrt{2}-7|<\frac{1}{10}.$$

$2\sqrt{2}-[2\sqrt{2}]$ 与 $7\sqrt{2}-[7\sqrt{2}]$ 都在 0.8 与 0.9 之间，所以

$$|(7\sqrt{2}-9)-(2\sqrt{2}-2)|<\frac{1}{10},\quad |5\sqrt{2}-7|<\frac{1}{10}.$$

8. $|4\sqrt{3}-7|<\frac{1}{10}$. q 是不超过 11 的二数之差.

9. $n+1$ 个数 $i\alpha-[i\alpha]$ $(i=1, 2, \cdots, n+1)$落在 n 个开区间 $\left(\frac{i-1}{n}, \frac{i}{n}\right)$ $(i=1, 2, \cdots, n)$中，所以有两个落在同一个区间内. 设它们对应着$i=j$，k，则 $|j\alpha-[j\alpha]-k\alpha+[k\alpha]|<\frac{1}{n}$，此即所需要的结论.

10. 在问题 9 中，$0<j$，$k\leqslant n+1$，所以 $|j-k|\leqslant n$，从而存在整数p，q，$q\leqslant n$，使得$|q\alpha-p|<\frac{1}{n}$. 此时$\left|\alpha-\frac{p}{q}\right|<\frac{1}{nq}<\frac{1}{q^2}$.

11. 属于 F_{n+1} 但不属于 F_n 的项，是 $\frac{k}{n+1}$，其中gcd $(k, n+1)=1$. 恰好有 φ $(n+1)$个这样的 k，所以 F_{n+1} 比 F_n 多 φ $(n+1)$项，由此及归纳法可得到 F_n 所含的项数.

12. $\frac{1}{2}$.

13. OCA 的面积等于 OCE 的面积，都是 $\frac{1}{2}$.

倘若把这两个三角形都看作以 OC 为底，那么从 A 和 E 到底边的高相等. 设 AE 与 OC 交于 M，则三角形 AMH 与 EMK 全等，所以 HK 的中点是 AE 的中点. 关于点 $M=(\frac{1}{2}(b+f), \frac{1}{2}(a+e))$的半周旋转使 A 和 E 交换位置，并且把 O 点映射成 $(b+f, a+e)$，又因为 M 在 OC 上，所以有 $\frac{a+e}{b+f}=\frac{c}{d}$.

14. 三角形$(0,0)$，(b,a)，(d, c)的面积是 $\frac{1}{2}$，所以平行四

边形$(0,0)$, $(b,a)(b+d,a+c)$, (d,c)的面积是1，而且问题中的两个三角形各占平行四边形的一半. 这三项在Farey数列F_{b+d}中是相邻的; 因为在连接$(0,0)$与$(b+d, a+c)$的线段上没有另外的格点, 所以它们不可能同时出现在前面的Farey数列中.

若$b+d\leqslant n$,那么$\frac{a}{b}$与$\frac{c}{d}$就不是F_n中的相邻项.

15. 连接$(0,0)$与$(b+d, a+c)$的线段是以$(0,0)$, (b,a)与$(0,0)$ (d,c)为边的平行四边形的对角线. 连接$(0,0)$与$(bu+d, au+c)$的线段是以$(0,0)$ (bu, au)与$(0,0)$ (d,c)为边的平行四边形的对角线.

16. 当$0<k<1$时, 对于任意实数r, s, 数$kr+(1-k)s$将它们按$\frac{1-k}{k}$的比例分开. 而且它们之间的任一数都是$kr+(1-k)s$ $(0<k<1)$的形式. (见问题9.31).

现在, 有

$$\frac{a}{b}\frac{bu}{bu+dv}+\frac{c}{d}\left(1-\frac{bu}{bu+dv}\right)=\frac{au+cv}{au+dv},$$

而且, 由于a, b, c, d, u, v都是正数, 所以

$$0<\frac{bu}{bu+dv}<1.$$

若r与s是有理数, 那么在它们之间的有理数都有$kr+(1-k)s$的形式, 此处k是有理数且$0<k<1$. 若k是给定的, 而且b和d也是给定的整数, 那么, 为了证明$\frac{a}{b}$与$\frac{c}{d}$之间的有理数都具有所给定的形式, 只要选取整数u, v, 使得$\frac{v}{u}=\frac{b}{dk}-\frac{b}{d}$即可.

17. 设$\frac{a}{b}$与$\frac{c}{d}$是某个Farey数列的相邻项, 则由问题

12，三角形(0,0)，(b, a)，(d, c)的面积是 $\frac{1}{2}$．设 $\frac{p}{q}$ 与 $\frac{a}{b}$ 是另一个 Farey 数列的相邻项，则三角形(0,0)，(b, a)，(q, p)的面积也是 $\frac{1}{2}$．因此，若 $\frac{c}{d}$ 与 $\frac{p}{q}$ 都比 $\frac{a}{b}$ 大或都比它小，那么连接(d, c)与(q, p)的直线平行于直线(0,0)(b, a)．由于在(d, c)与$(b+d, a+c)$之间没有格点，所以 $\frac{a+c}{b+d}$ 是 Farey 数列中介于 $\frac{a}{b}$ 与 $\frac{c}{d}$ 之间的第一项．

$$\left|\frac{a+c}{b+d}-\frac{a}{b}\right|=\left|\frac{bc-ad}{b\,(b+d)}\right|=\frac{1}{b\,(b+d)}\leqslant\frac{1}{b\,(n+1)}.$$

18．$\frac{1}{2}<\frac{1}{\sqrt{2}}<1$，$\frac{2}{3}<\frac{1}{\sqrt{2}}<1$，

$\frac{2}{3}<\frac{1}{\sqrt{2}}<\frac{3}{4}$，$\frac{2}{3}<\frac{1}{\sqrt{2}}<\frac{5}{7}$．

F_2：$\frac{1}{2}<\frac{1}{\sqrt{2}}<1$，大于中项．$\frac{a}{b}=1$．

F_3：$\frac{2}{3}<\frac{1}{\sqrt{2}}<1$，小于中项．$\frac{a}{b}=\frac{2}{3}$．

F_4, F_5, F_6：$\frac{2}{3}<\frac{1}{\sqrt{2}}<\frac{3}{4}$，小于中项．$\frac{a}{b}=\frac{2}{3}$．

F_7：$\frac{2}{3}<\frac{1}{\sqrt{2}}<\frac{5}{7}$，小于中项．$\frac{a}{b}=\frac{5}{7}$．

19．是的，因为根据问题17，0与1之间的每一数 $\frac{a}{b}$ 总是

与 Farey 数列 F_7 的某一项之差小于 $\frac{1}{8b}$.

20. 0与 1 之间的每一个数 $\frac{a}{b}$ 总是与 Farey 数列 F_n 中的某一项之差小于 $\frac{1}{b(n+1)}$.

21. 对于任意实数 α，存在整数 a,b，使得 $b \leqslant n$ 并且

$$\left|\alpha-[\alpha]-\frac{a}{b}\right| \leqslant \frac{1}{b(n+1)},$$

因而

$$\left|\alpha-\frac{b[\alpha]+a}{b}\right| \leqslant \frac{1}{b(n+1)}.$$

23. 1，2，3，5.

24. 当 $bp \neq qa$ 时，

$$\left|\frac{bp}{q}-a\right|=\left|\frac{bp-aq}{q}\right| \geqslant \frac{1}{q}.$$

25. 因为 α 是无理数，所以$\left|\alpha-\frac{a}{b}\right|>0$，因而存在某个整数 n，使得$\left|\alpha-\frac{a}{b}\right|>\frac{1}{n}$.

根据问题 20，存在整数 p,q，使得

$$\left|\alpha-\frac{p}{q}\right| \leqslant \frac{1}{q(n+1)}<\frac{1}{n}<\left|\alpha-\frac{a}{b}\right|, q \leqslant n.$$

显然$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}$. 这个过程可以反复进行，从而得到无限多对这样的整数.

26. $$\left|\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}\right|=\left|\frac{p_n q_{n-1}-q_n p_{n-1}}{q_n q_{n-1}}\right|=\frac{1}{q_n q_{n-1}},$$

并且

$$\left|\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}\right|>\left|\alpha-\frac{p_{n-1}}{q_{n-1}}\right|.$$

27.

0.414	6.120	14.668
1.657	11.647	2.479
0.728	5.002	12.119
2.627	11.186	22.587
0.355	3.198	8.883
2.912	10.039	20.008
6.296	0.708	4.962
2.510	8.205	16.743
6.551	16.531	0.354
1.421	5.685	12.792

$\sqrt{2}=[1,\dot{2}]$. 前五个渐近分数是 $\frac{1}{1}$, $\frac{3}{2}$, $\frac{7}{5}$, $\frac{17}{12}$, $\frac{41}{29}$.

$|\sqrt{2}-p/q|q^2=0.414, 0.343, 0.355, 0.353, 0.354$.

28. 因为$\sqrt{2}$ 在它的相邻渐近分数之间, 所以

$$\left|\sqrt{2}-\frac{p_n}{q_n}\right|+\left|\sqrt{2}-\frac{p_{n+1}}{q_{n+1}}\right|=\left|\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}\right|.$$

这说明, 两个相邻的渐近分数中, 至少有一个满足条件 $\left|\sqrt{2}-\frac{p}{q}\right|<\frac{1}{2q^2}$.

29. 将 $\sqrt{2}$ 换成任意无理数 α, 问题 28 的推理仍是正确的.

30. (i) $\sqrt{2}$ 在它的两个相邻的渐近分数之间, 由此, 与问题

28 的证明类似，可得到所要的结论. 因为 q_{n-1} 与 q_n 都是整数，所以等号不可能成立.

(ii) $y=x+\frac{1}{x}$ 是以 $x=0$ 与 $y=x$ 为渐近线的双曲线. 若 $x+\frac{1}{x}=\sqrt{5}$，则 $x=\frac{1}{2}(\sqrt{5}\pm1)$，而且，对于这两个数值之间的 x 值，有 $x+\frac{1}{x}<\sqrt{5}$. 由于 $\frac{1}{2}(\sqrt{5}-1)<1<\frac{1}{2}\cdot(\sqrt{5}+1)$，所以若 $x>1$ 且 $y<\sqrt{5}$，则 $x<\frac{1}{2}(\sqrt{5}+1)$，这与 $\frac{1}{x}>\frac{1}{2}(\sqrt{5}-1)$ 等价.

(iii) 由(i)得到

$$\sqrt{5}>\frac{q_n}{q_{n-1}}+\frac{q_{n-1}}{q_n}\text{ 且 }\sqrt{5}>\frac{q_{n+1}}{q_n}+\frac{q_n}{q_{n+1}}.$$

由于 $q_{n+1}>q_n>q_{n-1}\geqslant 1$，所以，由(ii)推出

$$\frac{q_{n-1}}{q_n}>\frac{1}{2}(\sqrt{5}-1)\text{ 且 }\frac{q_{n+1}}{q_n}<\frac{1}{2}(\sqrt{5}+1).$$

于是 $1+\frac{q_{n-1}}{q_n}>\frac{q_{n+1}}{q_n}$，$q_n+q_{n-1}>q_{n+1}$. 然而 $q_{n+1}=a_nq_n+q_{n-1}$，其中 $a_n\geqslant 1$，这就出现了矛盾.

31. 用 α 代替 $\sqrt{2}$ 后，上题的推理仍成立.

32. $[1,1,1,1]$

33. (i) $\left|\frac{1}{2}(\sqrt{5}+1)-\frac{p}{q}\right|=\frac{1}{cq^2}$

$$\Rightarrow\frac{1}{2}\sqrt{5}\,q\pm\frac{1}{cq}=p-\frac{1}{2}q$$

$$\Rightarrow 5q^2/4 \pm \sqrt{5}/c + \frac{1}{c^2q^2} = p^2 - pq + \frac{q^2}{4}$$

$$\Rightarrow \frac{1}{c^2q^2} \pm \frac{\sqrt{5}}{c} = p^2 - pq - q^2.$$

(ii) 若 $p^2 - pq - q^2 = 0$，则 $\left(\frac{p}{q}\right)^2 - \frac{p}{q} - 1 = 0$，于是 $\frac{p}{q} = \frac{1}{2}(1 \pm \sqrt{5})$，这与$\sqrt{5}$ 的无理性矛盾.

(iii) 若 $c > \sqrt{5}$，则当 $q^2 > \frac{1}{5}\left(1 - \frac{\sqrt{5}}{c}\right)$时，

$$-1 < \frac{1}{c^2q^2} \pm \frac{\sqrt{5}}{c} < 1.$$

(iv) 若 $c > \sqrt{5}$，由(iii)和(i)推出，除有限多个 q 外，应该有 $-1 < p^2 - pq - q^2 < 1$. 但是 p 与 q 都是整数，因此 $p^2 - pq - q^2$ 也是整数，由(ii)可知，这个条件是不能成立的.

当 $\frac{p}{q}$ 是 $\frac{1}{2}(\sqrt{5}+1)$的前十个渐近分数之一时，求出(i)中的 c 是有好处的.

此处的推理可用于对一类实数的逼近，它们的连分数中，除有限项外，都是由数码 1 组成的.

34. $\sqrt{2}$ 是无理数，所以不存在整数 p，q 使得 $p^2 - 2q^2 = 0$，因此

$$|p^2/q^2 - 2| = \left|\frac{p^2 - 2q^2}{q^2}\right| \geqslant \frac{1}{q^2}.$$

对于 $1 \leqslant x \leqslant 2$，连接$(x, x^2-2)$与$(\sqrt{2}, 0)$的弦的斜率当 $x=2$ 时取最大值.

对于任意的有理数 $\frac{s}{q} \neq 0$，存在介于 1 与 2 之间的 $\frac{p}{q}$，使得

$$\left|\frac{s}{q}-\sqrt{2}\right| \geqslant \left|\frac{p}{q}-\sqrt{2}\right| \geqslant (2-\sqrt{2})/2q^2 .$$

$$9>8 \Rightarrow 3>2\sqrt{2} \Rightarrow 4-2\sqrt{2}>1 \Rightarrow 2-\sqrt{2}>\frac{1}{2} .$$

由此可以断定，若从实轴上把每个有理点 $\frac{p}{q}$ 的半径为 $\frac{1}{4q^2}$ 的一个邻域去掉，则 $\sqrt{2}$ 不会被去掉.

35. 由问题 34 知，$q<4$. 若 $q=1$ ，则 $p=1$ 或 2 . 若 $q=2$ ，则 $p=3$. $\left|\frac{4}{3}-\sqrt{2}\right|$ 与 $\left|\frac{5}{3}-\sqrt{2}\right|$ 都大于 $\frac{1}{27}$.

由问题 34 知，$\frac{q}{c}<4$ ，所以 q 至多可取有限个值. 设 $n=\left[\sqrt{2}+\frac{c}{q^3}\right]+1$ ，则只需考虑在 $\pm nq$ 之间的那些 p .

36. 对于 $1\leqslant x\leqslant 2$，连结 (x, x^2-3) 与 $(\sqrt{3}, 0)$ 的线段当 $x=2$ 时有最大斜率. 由此及 $\left|\frac{p^2}{q^2}-3\right|>\frac{1}{q^2}$，推出 $\left|\frac{p}{q}-\sqrt{3}\right| \geqslant (2-\sqrt{3})/q^2$.

由 $81>75 \Rightarrow 9>5\sqrt{3} \Rightarrow 10-5\sqrt{3}>1 \Rightarrow 2-\sqrt{3}>\frac{1}{5}$.

于是 $\frac{c}{q^3}>\left|\frac{p}{q}-\sqrt{3}\right|>\frac{1}{5q^2} \Rightarrow 5c>q$ ，因而只需考虑有限个整数 q .

37. 对于 $1\leqslant x\leqslant 2$ ，连结 (x, x^2-x-1) 与 $\left(\frac{1}{2}(\sqrt{5}+1), 0\right)$

的线段的斜率当 $x=2$ 时取最大值. 因而都不超过

$$1\Big/\left[2-\frac{1}{2}(\sqrt{5}+1)\right].$$

$$49>45\Rightarrow 7>3\sqrt{5}\Rightarrow 9-3\sqrt{5}>2\Rightarrow\frac{1}{2}(3-\sqrt{5})>\frac{1}{3}.$$

请将本题结果与问题 33 比较.

38. 设 $\sqrt[3]{2}$ 等于某个有理数，它的素因数分解式(问题10.5)是 $p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$，则

$$2=p_1^{3a_1}p_2^{3a_2}, \cdots p_n^{3a_n}.$$

但这是不可能的. 因此对于任何非零整数 p, q，总有 $p^3-2q^3\neq 0$，从而 $|p^3/q^3-2|\geqslant\dfrac{1}{q^3}$.

$y=x^3-2$ 的图形，当 $1<x<2$ 时是凹的. 因此，在此区间中，连结 $(\sqrt[3]{2},0)$ 与 (x, x^3-2) 的线段的斜率当 $x=2$ 时取最大值，从而都是小于或等于 $6/(2-\sqrt[3]{2})$.

$$27>16\Rightarrow 3>2\sqrt[3]{2}\Rightarrow 4-2\sqrt[3]{2}>1\Rightarrow 24-12\sqrt[3]{2}>6$$

$$\Rightarrow\frac{1}{6}(2-\sqrt[3]{2})>\frac{1}{12}.$$

再仿照问题 35 作其余的论证.

39. 若 $\dfrac{1}{3}(2-\sqrt[3]{2})=r$ 是有理数，那么 $\sqrt[3]{2}=2-3r$ 就成了有理数，这与问题 38 矛盾.

因为 $(2-3r)^3=2$，所以 $-27r^3+54r^2-36r+8=2$，$9r^3-18r^2+12r-2=0$. 我们来考察 $y=9x^3-18x^2+12x-2$ 的图形. 由于

$$\frac{dy}{dx}=27x^2-36x+12=3(3x-2)^2,$$

曲线的斜率总是非负的，所以它与x轴仅有一个交点. 因此方程$y=0$不存在有理根，即$9p^3/q^3-18p^2/q^2+12p/q-2\neq 0$.

当$0<x<\frac{2}{3}$时曲线是凸的，当$\frac{2}{3}<x<1$时曲线是凹的. 方程的根接近于0.25. 所以当$0<x<1$时，以$\left(\frac{1}{3}(2-\sqrt[3]{2}),0\right)$和$(0,-2)$为端点的线段有最大斜率. 这和问题38中的弦的最大斜率相同，以后的推算也是类似的.

40. 显然，此处所涉及的，是一个整数除以q^n，因此，只需证明这个整数不等于零. 若它是零，那么有理数$\frac{p}{q}$就是方程的根，因而这个多项式有因式$px-q$，α就满足一个次数为$n-1$的方程了.

41. $A\geqslant|f'(x)|\geqslant\frac{|f(b)|}{|b-\alpha|}$.

42. 对于任意正整数p与q，存在整数p'，使得$\alpha-\frac{1}{2}\leqslant p'/q\leqslant\alpha+\frac{1}{2}$，而且，若$\frac{p}{q}$不属于这个区间，则

$$\left|\frac{p}{q}-\alpha\right|>\left|\frac{p'}{q}-\alpha\right|,$$

因此只需考虑$\frac{p}{q}$属于区间$\left[\alpha-\frac{1}{2},\alpha+\frac{1}{2}\right]$的情形. 设$f(x)$是整系数多项式且$f(\alpha)=0$，记$|f'(x)|$在此区间中的最大值为$A$. 先用问题41，再用问题40即可得证.

历 史 注 记

问题 9 的证明使用了 P.G.L.Dirichlet 的“鸽巢原则”：若将 $n+1$ 个元素放入 n 个集合中，则至少有一个集合含有其中的两个或两个以上的元素. 1891 年，J.Hurwitz 利用 Farey 数列，而不是利用连分数，证明了他的关于无理数的有理逼近的定理. 1903 年，E.Borel 指出，无理数的连分数的每三个相邻的渐近分数中，至少有一个满足 Hurwitz 定理中的条件. 我们这里的证明，是由 O.Perron (1910)给出的. 1851 年，J.Liouville 构造了第一批可以给出证明的超越数. 1873 年，C.Hermite 证明了数 e 的超越性，而在 1882 年，F.Lindemann 则证明了数 π 的超越性.

参 考 书 目

Andrews, G. E., *Number theory*, Saunders, 1971.

第十二章与第十三章是关于分拆的内容，可与我们的第七章同时阅读.

Bell, E. T., *The last problem*, Gollancz, 1962.

选收了自 Fermat 的信件以来的文献资料，很有意义.

Bolker, E. D., *Elementary number theory*, Benjamin, 1970.

使用了群，环，域的知识；可与我们的第四，五，六章同时阅读.

Butts, T., *Problem solving in mathematics*, Scott-Foresman, 1973.

一本初级读物，适于作为预备知识，可与我们的第一章同时阅读.

Chrystal, G., *Algebra* (Ⅱ), Chelsea, 1964.

某些章节可与我们的第七章和第十章同时阅读.

Davenport, H., *The higher arithmetic*, Hutchinson, 1968.

特别要推荐此书与我们这书同时阅读.

Dickson, L. E., *History of the theory of numbers* (共三卷), Chelsea, 1950.

广泛而又详细的参考文献.

Edwards, H. M., *Fermat's last theorem, a genetic introduction to algebraic number theory*, Springer, 1977.

按历史的顺序，讨论了丰富的数学内容；学完入门之后，就能很好地评价它了. 但是，从我们的第五章和第六章就可开始同时阅读.

Hardy, G. H. 与 Wright, E. M., *An introduction to the theory of numbers* (第五版), Oxford, 1980.

大学数论课程的经典参考书；对初学者来说比较难读，但其中的第三章例外(可与我们的第九章同时阅读).

Hubbard, R. L., *The factor book*, Hilton Management Services, 1975.

提供了不超过 100000 的整数的素因数.

LeVeque, W. J., *Topics in number theory*, Addison-Wesley, 1956.

第一卷适于作为关于算术函数与素数分布的进一步的读物；第二卷适于作为关于二次型的进一步的读物.

Mathews ,G .B . , *Number theory* , Chelsea , (无日期)

有二次互反律的几个证明，是关于二次型的进一步的读物.

Nagell , T . , *Introduction to number theory* , Chelsea , 1964 .

给出了 Legendre 定理的三个不同形式.

Niven , I . , *Numbers rational and irrational* , Mathematical Association of America , 1961 .

对初学者来说，是本书第十一章的引论，它也以我们所构造的超越数为其结尾.

Niven , I . , *Irrational numbers* , Carus series , Mathematical Association of America ,1967 .

关于我们的第十一章的进一步读物.

Niven , I . 与 Zuckerman , H .S . , *An introduction to the theory of numbers* (第三版), Wiley , 1972 .

是一本好的常用教科书，有练习题，包括了入门的大部分内容.

Olds , C . D . , *Continued fractions* , Mathematical Association of America , 1963 .

特别要推荐与我们的第十章同时阅读.

Ore , O . , *Number theory and its history* , McGraw－Hill , 1948 .

可与我们的第二，三，六章同时阅读.

Ore, O . , *Invitation to number theory* , Mathematical Association of America , 1967 .

可与我们的第一章同时阅读.

Pollard , H . 与Diamond , H . G . , *The theory of algebraic numbers* (第二版), Garus series, Mathematical Association of America , 1975 .

关于我们的第五章的进一步读物.

Polya, G . 与 Szegö , G . , *Problems and theorems in analysis* (Ⅱ), Springer , 1976 .

第八部分研究较高深的数论内容，写作风格和入门相似.

Reid , C . , *From zero to infinity* ,Routledge and Kegan Paul , 1956 .

对于打算学习入门的初学者来说，这本书使他们真正体会一下数论的趣味.

Roberts, J., *Elementary number theory, a problem oriented approach*, M.I.T., 1977.

与入门使用一系列问题相比, 此书讲得较深、较快.

Shanks, D., *Solved and unsolved problems in number theory* (第二版), Chelsea, 1978.

可与我们的第三, 四, 五, 六, 十章同时阅读.

Sierpinski, W., *Pythagorean triangles*, Graduate School of Science, Yeshiva University, New York, 1962.

可与我们的第五章第一部分同时阅读.

Stark, H.M., *An introduction to number theory*, M.I.T., 1978.

第七章用几何的方法处理连分数, 这是由 F.Klein 首先提出的.

Weil, A., *Number theory for beginners*, Springer, 1979.

叙述简明扼要, 使用了近世代数的语言. 可与我们的第二章同时阅读.

定义与定理

第 一 章

除法算式 (1.24)

设 a 与 b 是非零整数，则存在唯一确定的整数 q，r，使得

$$a=bq+r, \quad 0\leqslant r<|b|.$$

定义：最大公约数 (1.34)

若 a 和 b 是非零整数，d 是使 $d|a$ 与 $d|b$ 成立的最大正整数，则 $d=\gcd(a,b)$.

Euclid 算法 (1.34，1.39)

设 $d=\gcd(a,b)$，则存在整数 x，y，使得 $d=ax+by$.

定义：素数 (1.43)

若 p 是给定的异于 1 的正整数，并且由 $a|p$ 可推出 $a=\pm 1$，$\pm p$，则称 p 是素数.

算术基本定理 (1.58)

大于 1 的正整数都可以写成 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，其中 $k\geqslant 1$，p_i 是不相同的素数，α_i 是唯一确定的正整数.

定理 (1.64)

素数的个数无限.

第 二 章

定义：剩余类 (2.3)

称整数集合 $\{x:n|x-a\}$ 是模 n 的一个剩余类. 用 $\mathbf{Z}_n$ 表示模 n 的 n 个剩余类所成的集合. 当 x 与 y 属于模 n 的同一个剩余类时，记为 $x\equiv y \pmod{n}$.

中国剩余定理 (2.18)

设 m_1，m_2，…，m_n 两两互素，则同余方程组

$$x \equiv a_i \pmod{m_i}, i=1,2,\cdots,n$$

有唯一解 $(\bmod\ m_1 m_2 \cdots m_n)$.

定义：模加法 (2.26)

若整数 a 属于模 n 的剩余类 $[a]$，整数 b 属于模 n 的剩余类 $[b]$，则定义 $\mathbf{Z}_n$ 上的模加法为 $[a]+[b]=[a+b]$.

定义：Euler 的 φ 函数 (2.39)

$\varphi(n)$等于群 $(\mathbf{Z}_n+)$的生成元个数. 另一个等价的定义是：$\varphi(n)$是从 1 到 n 的整数中与 n 互素的整数个数.

定理：φ 是积性函数 (2.50)

设 m 与 n 互素，则 $\varphi(mn)=\varphi(m)\varphi(n)$.

定理：$\varphi(n)$的值 (2.53)

设 $p_1, p_2, \cdots, p_k$ 是 n 的不同的素因数，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

定理 (2.64)

$$\sum_{d|n}\varphi(d)=n .$$

第 三 章

定义：模乘法 (3.5)

若整数 a 属于模 n 的剩余类 $[a]$，整数 b 属于模 n 的剩余类 $[b]$，则定义 $\mathbf{Z}_n$ 上的模乘法为 $[a][b]=[ab]$.

Fermat 定理 (3.19)

对于任意整数 x 与任意素数 p，有 $x^p \equiv x \pmod p$.

Wilson 定理 (3.25)

对于任意素数 p，有 $(p-1)! \equiv -1 \pmod p$.

定理：一次同余方程 (3.33)

设 $d=\gcd(a, n)$，则当 $d\,|\,b$ 时，$ax \equiv b \pmod n$有解；否则无解. 若有解，则有 d 个对模 n 不同余的解.

定义 (3.36)

用 $\mathbf{M}_n$ 表示 $\mathbf{Z}_n$ 中可逆元素的集合，就是说，$\mathbf{M}_n$ 由 $\mathbf{Z}_n$ 的这种元素组成：它们在$(\mathbf{Z}_n, \times)$中有逆元素. 从 $\mathbf{M}_n$ 的每个剩余类中取一个整数，就构成模 n

的一个简化剩余系.

定理 (3.36)

$|\mathbf{M}_n|=\varphi(n)$.

Fermat－Euler 定理 (3.41)

设 a 与 n 互素, 则 $a^{\varphi(n)}\equiv 1 \pmod{n}$.

关于多项式的Lagrange 定理 (3.57)

域上的 n 次多项式至多有 n 个不同的零点.

定义：原根 (3.62)

若 $[a]$ 是群 $(\mathbf{M}_n,\times)$ 的一个生成元, 则称整数 a 是模 n 的一个原根.

定理 (3.61, 3.65, 3.74)

设 n 是一个奇数的幂, 或是这样一个幂乘以 2, 则存在模 n 的原根.

Chevalley 定理 (3.87)

最高次数小于 n 的整系数 n 元多项式, 若其常数项为零, 则必有非平凡解 $(\bmod\, p)$.

第 四 章

定义：二次剩余 (4.3, 4.8)

若 $[a]$ 是群 $(\mathbf{M}_n,\times)$ 中的一个平方, 则称 a 是对模 n 的二次剩余, 否则称 a 是对模 n 的二次非剩余.

定义：Legendre 符号 (4.15)

对于素数 p, 当 a 是对模 p 的二次剩余时, 令 $\left(\frac{a}{p}\right)=+1$; 当 a 是对模 p 的二次非剩余时, 令 $\left(\frac{a}{p}\right)=-1$; 在其他情形, 则令 $\left(\frac{a}{p}\right)=0$.

定理 (4.14, 4.15, 4.41)

$$\left(\frac{a}{p}\right)\equiv a^{\frac{1}{2}(p-1)} \pmod{p},$$

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad \left(\frac{2}{p}\right)=(-1)^{\frac{1}{8}(p^2-1)}.$$

定理 (4.18)

设 p 是奇素数, 则当 $p\equiv 1 \pmod{4}$ 时, -1 是对模 p 的二次剩余; 当

$p\equiv 3 \pmod 4$时，-1是对模p的二次非剩余.

Gauss 引理 (4.43)

设p是奇素数，a是整数但不是p的倍数，则$\left(\frac{a}{p}\right)=(-1)^l$，其中$l$是与

$$a\cdot 1\ ,\ a\cdot 2\ ,\cdots,\ a\cdot\frac{1}{2}(p-1)$$

同余的绝对最小剩余中负号的个数.

二次互反律 (4.62)

设p与q是不同的奇素数，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{4}(p-1)(q-1)}.$$

第 五 章

定义：Pythagoras 三元数组 (5.5)

若x, y, z都是整数且$x^2+y^2=z^2$，则称(x, y, z)是一个Pythagoras三元数组. 此外，若$\gcd(x, y, z)=1$，则称这个三元数组是本原三元数组.

定理：Pythagoras 三元数组定理 (5.15)

设(x, y, z)是一个本原Pythagoras三元数组，则x与y中有一个偶数. 当x是偶数时，$x=2pq$，$y=p^2-q^2$，$z=p^2+q^2$，其中p与q是互素整数.

定义：递降法 (注记5.20)

Fermat所提出的对良序原则的一个应用.

定理 (5.21)

方程$x^4+y^4=z^4$没有非零整数解.

定理 (5.68)

方程$x^3+y^3=z^3$没有非零整数解.

第 六 章

定理 (6.10, 6.11, 6.12)

设p是素数，$p|x^2+y^2$，而且x与y都不被p整除，则$p=2$或$p\equiv 1 \pmod 4$.

设q是素数，$q\equiv 3 \pmod 4$而且$q|x^2+y^2$，则在x^2+y^2的素因数分解

式中，q 的指数是偶数.

定理 (6.15)

$$(a^2+b^2)(c^2+d^2)=(ad-bc)^2+(ac+bd)^2 .$$

定理 (6.33，6.36)

同余于 1 (mod 4)的素数可以唯一地表示成二平方之和.

定理 (6.34)

一个正整数可以表为二平方之和的充要条件是，在它的素因数分解式中，同余于 3 (mod 4)的素因数的指数是偶数.

Lagrange 四平方定理 (6.40)

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)\\ &=(ax-by-cz-dt)^2+(ay+bx+ct-dz)^2\\ &\quad+(az-bt+cx+dy)^2+(at+bz-cy+dx)^2 .\end{aligned}$$

定理 (6.51)

素数都可以表示为四平方之和.

定理 (6.52)

正整数都可以表示为四平方之和.

定理 (6.54)

形如 $4^h(8k+7)$的正整数不能表示为三平方之和.

第　七　章

定义：分拆 (7.1)

若 n 是一组正整数之和，则称这个和式中分量的全体为 n 的一个分拆.

定义：Ferrers 图 (7.2)

即分拆图，是一个点列，其中每一列表示一个部分数，而且左边一列的点数不比右边一列的少.

定义：共轭分拆 (7.3)

若某个分拆图可以通过将另一个分拆图的行与列转置而得到，则称这两个分拆是共轭的.

定义：生成函数 (7.16)

称形式幂级数 $f(x)=1+\sum_{n=1}^{\infty}a_n x^n$ 是序列 (a_n)的生成函数.

定义 $p_m(n)$ (7.22)

在n的分拆中，部分数不超过m的那种分拆的个数，记作$p_m(n)$.

定理 (7.22)

$(p_m(n))$的生成函数是

$$\frac{1}{(1-x)(1-x^2)\cdots(1-x^m)} .$$

Euler 定理 (7.47)

$$(1-x)(1-x^2)\cdots(1-x^n)\cdots=\sum_{n=-\infty}^{\infty}(-1)^n x^{\frac{1}{2}n(3n-1)} .$$

第 八 章

定理 (8.9)

线性变换 $(x,y)\to(x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 将 $\mathbf{Z}^2$ 满射到 $\mathbf{Z}^2$ 的充要条件是：a，b，c，d是满足 $ad-bc=\pm 1$ 的整数.

定义：幺模变换 (8.15)

$\mathbf{R}^2$ 中的线性变换若将 $\mathbf{Z}^2$ 满射到 $\mathbf{Z}^2$，则称为幺模变换.

定义：幺模矩阵 (8.15)

若$(x,y)\to(x,y)A$ 是幺模变换，则称 A 为幺模矩阵.

定义：等价二次型 (8.25)

若$(x,y)\to(px+ry,\ qx+sy)$是幺模变换，则称 $ax^2+bxy+cy^2$ 与 $a(px+ry)^2+b(px+ry)(qx+sy)+c(qx+sy)^2$ 是等价的二次型.

定理 (8.25)

等价二次型有相同的值集合.

定义：判别式 (8.37)

二次型 $ax^2+bxy+cy^2$ 的判别式是 b^2-4ac.

定理 (8.37)

等价二次型的判别式相等.

定义：定型 (8.38)

二次型 $ax^2+bxy+cy^2$，当 $b^2-4ac<0$ 且 $a>0$ 时，称为正定的；当 $b^2-4ac<0$ 且 $a<0$时，称为负定的；当 $b^2-4ac>0$时，称为不定的.

定义：**正规表示** (8.48)

若 $n=ap^2+bpq+cq^2$ 且 $\gcd(p,q)=1$ 或者 $\{|p|,|q|\}=\{0,1\}$，则称整数 n 由 $ax^2+bxy+cy^2$ 正规表示.

定理 (8.49，8.50)

整数 n 可以由 $ax^2+bxy+cy^2$ 正规表示的充要条件是，存在一个等价二次型，它的 x^2 项系数是 n.

定义 (8.57)

若 $0\leqslant b\leqslant a\leqslant c$，则称正定二次型 $ax^2+bxy+cy^2$ 是约化二次型.

定理：等价的标准型 (8.56，8.66)

每个正定二次型只与一个约化二次型等价.

定义：**自守变换** (8.73)

二次型的自守变换是指把这个二次型变换为自身的幺模变换.

定理 (8.77)

正定二次型的自守变换群，不是 2 阶循环群，就是阶为 4，8 或 12 的二面体群.

第　九　章

定义：**基本平行四边形** (9.5)

若 $\mathbf{Z}^2$ 的子群 G 是由 (a,b) 与 (c,d) 生成的，并且这两个有序数对互不是另一个的倍数，则称以 $(0,0)$，(a,b)，(c,d)，$(a+c,b+d)$ 为顶点的平行四边形是 G 的基本平行四边形.

定理 (9.23)

设 G 是 $\mathbf{Z}^2$ 的子群，Π 是它的基本平行四边形，则 G 在 $\mathbf{Z}^2$ 中的指数等于 Π 的面积.

Minkowski 定理 (9.39)

$\mathbf{R}^2$ 中的一凸的开集，若它关于 $(0,0)$ 对称，并且面积大于 4，则除点 $(0,0)$ 外，它必还含有 $\mathbf{Z}^2$ 的点.

定义：**基本平行六面体** (9.57)

若 $\mathbf{Z}^3$ 的子群 G 是由 $A=(a_1,a_2,a_3)$，$B=(b_1,b_2,b_3)$，与 $C=(c_1,c_2,c_3)$ 生成的，而且 $aA+bB+cC=(0,0,0)$ 仅当 $a=b=c=0$ 时成立，则称以 $(0,0,0)$，A，B，C，$B+C$，$C+A$，$A+B$，$A+B+C$ 为顶点的平行六面体是 G 的基本平行六面体.

定理 (9.66)

设 G 是 $\mathbf{Z}^3$ 的子群，Π 是它的基本平行六面体，则 G 在 $\mathbf{Z}^3$ 中的指数等于 Π 的体积.

Minkowski 定理 (9.71)

R^3 中的任一凸的开区域，若它关于(0, 0, 0)对称，体积大于 8，那么它必含有 $\mathbf{Z}^3$ 的点，但异于(0, 0, 0).

Legendre 定理 (9.86)

设在 a, b, c 的素因数分解式中，都不出现平方数，并且它们两两互素，又设 $ax^2+by^2+cz^2\equiv 0 \pmod{4abc}$ 有解 (x_1, y_1, z_1)，使得 $\gcd(ax_1, by_1, cz_1, 4abc)=1$，则 $ax^2+by^2+cz^2=0$ 有非零整数解.

第 十 章

定理 (10.6)

设 a 是非平方有理数，则 $\sqrt{a}$ 是无理数.

定义 (10.10)

$$[a_1, a_2, a_3, \cdots]=a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots}},$$

其中 a_i 都是实数，并且当 $i>1$ 时，$a_i\geqslant 1$.

定理 (10.13)

设 $[a_1, a_2, a_3, \cdots, a_k]=p_k/q_k$，则当 $n\geqslant 3$ 时，

$$\frac{p_n}{q_n}=\frac{a_n p_{n-1}+p_{n-2}}{a_n q_{n-1}+q_{n-2}}.$$

定义：渐近分数 (10.18)

若 $k\leqslant n$，则称 p_k/q_k 是 $[a_1, a_2, \cdots, a_n]$ 的第 k 个渐近分数.

定理 (10.22)

每个有理数只可能与两个不同形式的连分数相等，其中一个的项数是奇数，另一个的项数是偶数.

定理 (10.23, 10.24, 10.25)

每个无理数 x 只能有一个连分数表示式，它的渐近分数序列收敛于 x. 项数无限的连分数都是从无理数产生的.

定义：二次无理数与共轭数 (10.52)

一个无理数若满足某个整系数二次方程，则称为二次无理数. 这个方程的另一个解称为这个无理数的共轭数.

定理 (10.37, 10.53)

每个纯循环连分数对应着一个大于1的二次无理数，它的共轭数是大于 -1 的负数；反之亦然.

Pell 方程 (10.61)

设 $\sqrt{d}$ 的连分数的周期长度是 n，则 $p_n^2-dq_n^2=(-1)^n$，其中 p_n/q_n 是 $\sqrt{d}$ 的连分数的第 n 个渐近分数.

关于二次无理数的 Lagrange 定理 (10.76, 10.77)

二次无理数的连分数都是混循环的；反之亦然.

定理*(10.81, 10.82)

设 a, b 是互素的正整数，则二次型 ax^2-by^2 的全体自守变换构成一个无限循环群.

第十一章

定理 (11.10, 11.22)

对于任意的实数 α 与任意的正整数 n，可以找到整数 p, q，使得 $0<q\leqslant n$ 并且 $\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}$.

Hurwitz 定理 (11.31)

设 α 是无理数，则 α 的连分数的每三个相邻的渐近分数中，至少有一个使 $\left|\alpha-\frac{p}{q}\right|<\frac{1}{\sqrt{5}\,q^2}$ 成立.

Liouville 定理 (11.42)

设 α 是 $n(\geqslant 2)$ 次代数数，则存在正实数 A，使得 $\left|\alpha-\frac{p}{q}\right|>\frac{1}{Aq^n}$ 对于一切整数 p 及一切正整数 q 成立.

索　引

括号内是英文原文.

前缀"n"表示"注记", 若无"n", 则数字都是指的问题(例如 2.25, 等等).

英汉人名对照表

Chevalley	柴瓦里
Dirichlet	狄利克雷
Eratosthenes	厄拉多塞
Euclid	欧几里得
Euler	欧拉
Farey	法雷
Fermat	费马
Ferrers	费乐斯
Gauss	高斯
Hurwitz	胡尔维茨
Lagrange	拉格朗日
Legendre	勒让得
Liouville	刘维尔
Mersenne	麦尔森
Minkowski	闵可夫斯基
Pell	派尔
Pythagoras	毕达哥拉斯
Wilson	威尔逊